

notas para a unidade curricular

Tópicos de Matemática Discreta

mestrado integrado em Engenharia Informática

Universidade do Minho 2017/2018

Cláudia Mendes Araújo

Carla Mendes

Suzana Mendes Gonçalves

Capítulo 1

Noções elementares de lógica

1.1 Introdução

A palavra **lógica** tem raiz no grego clássico: *logos* significa *razão*.

A lógica consiste no estudo dos princípios e das técnicas do raciocínio, procurando definir linguagens formais que permitam representar de forma precisa e sem ambiguidade a linguagem natural e definindo regras que permitam a construção rigorosa e sistemática de argumentos válidos.

Desempenha, pois, um papel fundamental em qualquer área do saber, em particular na Matemática e na Informática.

Na Informática, a lógica é usada, por exemplo, no desenvolvimento de linguagens de programação, na verificação da correção de programas e nos circuitos digitais.

[Exemplo]

Consideremos as seguintes situações:

situação 1: Todos os coelhos gostam de cenouras. Este animal é um coelho. Então, este animal gosta de cenouras.

situação 2: Todos os que estão nesta sala gostam de Matemática. Tu estás nesta sala. Então, tu gostas de Matemática.

Formalmente, o raciocínio das duas situações é o mesmo: assumindo que todos os elementos x de um dado universo U satisfazem uma dada propriedade p e considerando um elemento x_0 de U , podemos concluir que x_0 satisfaz p . Note-se que é precisamente sobre o raciocínio, e não sobre o contexto em si, que o estudo da lógica vai debruçar-se.

Procurando estruturar raciocínios, podemos encontrar ferramentas eficazes na resolução de problemas, que podem ir de uma simples charada a problemas complexos das mais variadas áreas das ciências e da engenharia.

[Exemplo]

Consideremos o seguinte problema:

Um crime foi cometido por uma e apenas uma pessoa de um grupo de cinco suspeitos: Armando, Bernardo, Carlos, Daniel e Eduardo.

Questionados sobre quem era o culpado, cada um deles respondeu:

Armando: “Sou inocente.”

Bernardo: “O Armando disse a verdade.”

Carlos: “O Eduardo é o culpado.”

Daniel: “O Carlos mentiu.”

Eduardo: “O Daniel é o culpado.”

Sabendo que apenas um dos suspeitos mentiu e que todos os outros disseram a verdade, quem é o culpado?

A abordagem ao problema é claramente importante na eficiência da sua resolução. Fazendo uma leitura de todos os depoimentos, rapidamente percebemos que os depoimentos de Carlos e de Eduardo não podem ser ambos verdadeiros, uma vez que o crime foi cometido por uma e apenas uma pessoa. Se Carlos não mentiu, tanto Daniel como Eduardo mentiram, o que sabemos não ter acontecido, já que apenas um dos suspeitos mentiu. Sendo assim, Carlos mentiu e todos os outros disseram a verdade. Logo, Daniel é o culpado.

Para exprimir argumentos precisos e rigorosos sobre afirmações é indispensável uma linguagem simples e clara, na qual as afirmações efetuadas não tenham significado ambíguo.

A linguagem corrente não tem estes requisitos e torna-se necessário utilizar uma **linguagem formal**. Nesse sentido, adotamos um **sistema lógico** adequado. Um sistema lógico apresenta as seguintes componentes:

sintaxe - conjunto de símbolos e regras de formação que definem as palavras, designadas por *fórmulas*, que podem ser utilizadas para representar de forma precisa, concisa e sem ambiguidade a linguagem natural (ou parte dela);

semântica - conjunto de regras que associam um *significado* às fórmulas;

sistema dedutivo - conjunto de fórmulas, designadas por *axiomas*, e de regras, designadas por *regras de inferência*, utilizados na construção de argumentos.

Ao longo dos anos, foram definidos diversos sistemas lógicos. Nesta unidade curricular, estudaremos algumas noções básicas associadas ao **Cálculo Proposicional Clássico** e ao **Cálculo de Predicados Clássico**.

1.2 Cálculo Proposicional Clássico

1.2.1 Sintaxe

Na linguagem natural, podemos encontrar diversos tipos de frase – declarativas, exclamativas, interrogativas, imperativas. Na construção de um argumento, recorreremos apenas a frases declarativas.

As frases podem ser simples ou compostas.

Uma **frase (declarativa) simples** tem, gramaticalmente falando, um sujeito e um predicado.

[Exemplo]

As seguintes frases são frases simples.

Braga possui 181 954 habitantes no seu concelho.

O António gosta de Lógica.

Todo o número inteiro é par.

No Cálculo Proposicional (CP), cada frase simples é encarada como um elemento indivisível, não se diferenciando partes da afirmação como o nome ou o verbo.

[Definição 1.1] Representaremos as frases simples por $p_0, p_1, \dots, p_n, \dots$, com $n \in \mathbb{N}_0$. A estes símbolos chamamos **variáveis proposicionais** e denotaremos o conjunto das variáveis proposicionais por \mathcal{V}^{CP} .

A partir de frases simples e recorrendo a expressões como “não”, “e”, “ou”, “se... então”, “... se e só se...”, obtêm-se frases mais complexas, designadas por **frases compostas**.

[Exemplo]

As seguintes frases são frases compostas.

Braga possui 181 954 habitantes no seu concelho e conta com mais de 2000 anos de história como cidade.

Se o António gosta de Lógica, então é bom aluno a Tópicos de Matemática Discreta e a Lógica Computacional

Se todo o número inteiro é par, então 7 é divisível por 2.

No Cálculo Proposicional, as frases compostas são representadas usando:

- as variáveis proposicionais;
- os símbolos \perp , \neg , \wedge , \vee , \rightarrow e \leftrightarrow , chamados **conetivos proposicionais**, e designados, respetivamente, por **absurdo**, **negação**, **conjunção**, **disjunção**, **implicação** e **equivalência**;
- os parêntesis esquerdo e direito (e), chamados **símbolos de pontuação**.

Representemos por p_n e p_m duas frases declarativas ($n, m \in \mathbb{N}_0$).

A frase “não p_n ” designa-se por **negação de p_n** e é representada por $(\neg p_n)$. A $(\neg p_n)$ também podemos associar as leituras “é falso p_n ” e “não é verdade p_n ”.

A frase “ p_n e p_m ” designa-se por **conjunção de p_n e p_m** e é representada por $(p_n \wedge p_m)$. Nalguns contextos pode aparecer também na forma “ p_n mas p_m ”.

A frase “ p_n ou p_m ” designa-se por **disjunção de p_n e p_m** e é representada por $(p_n \vee p_m)$.

A frase “Se p_n , então p_m ” designa-se por **implicação de p_n , p_m** e é representada por $(p_n \rightarrow p_m)$. A $(p_n \rightarrow p_m)$ também podemos associar as leituras “ p_n implica p_m ”, “ p_n é condição suficiente para p_m ”, “ p_m é condição necessária para p_n ”, “ p_m se p_n ”, “ p_m sempre que p_n ”, “ p_n só se p_m ” e “ p_n somente se p_m ”. A p_n chamamos **antecedente** ou **hipótese** da implicação e a p_m chamamos **consequente** ou **conclusão**.

A frase “ p_n se e só se p_m ”, que resulta da conjunção das implicações “Se p_n , então p_m ” e “Se p_m , então p_n ”, designa-se por **equivalência de p_n e p_m** e é representada por $(p_n \leftrightarrow p_m)$. A $(p_n \leftrightarrow p_m)$ também se associam as leituras “ p_n é equivalente a p_m ” e “ p_n é necessário e suficiente para p_m ”.

[Exemplo]

Consideremos as seguintes frases e as variáveis proposicionais que as representam:

- p_0 : Braga possui 181 954 habitantes no seu concelho.
- p_1 : Braga conta com mais de 2000 anos de história como cidade.
- p_2 : O António gosta de Lógica.
- p_3 : O António é bom aluno a Tópicos de Matemática Discreta.
- p_4 : O António é bom aluno a Lógica Computacional.
- p_5 : Todo o número inteiro é par.
- p_6 : 7 é divisível por 2.

As frases compostas referidas no exemplo anterior podem ser representadas, respetivamente, por:

- [1] $(p_0 \wedge p_1)$
- [2] $(p_2 \rightarrow (p_3 \wedge p_4))$
- [3] $(p_5 \rightarrow p_6)$

Estipulados os símbolos que definem o alfabeto da linguagem do Cálculo Proposicional, podemos, agora, definir as palavras desta linguagem.

[Definição 1.2] O conjunto \mathcal{F}^{CP} das **fórmulas do Cálculo Proposicional** é o conjunto definido indutivamente pelas seguintes regras:

- (F_1) \perp é uma fórmula do CP;
- (F_2) toda a variável proposicional é uma fórmula do CP;
- (F_3) se φ é uma fórmula do CP, então $(\neg\varphi)$ é uma fórmula do CP;
- (F_4) se φ, ψ são fórmulas do CP, então $(\varphi \wedge \psi)$ é uma fórmula do CP;
- (F_5) se φ, ψ são fórmulas do CP, então $(\varphi \vee \psi)$ é uma fórmula do CP;
- (F_6) se φ, ψ são fórmulas do CP, então $(\varphi \rightarrow \psi)$ é uma fórmula do CP;
- (F_7) se φ, ψ são fórmulas do CP, então $(\varphi \leftrightarrow \psi)$ é uma fórmula do CP.

[Exemplo]

[1] A palavra $((\neg p_0) \rightarrow (p_1 \wedge p_2))$ é uma fórmula do Cálculo Proposicional, uma vez que:

- i. Pela regra (F_2), as variáveis proposicionais p_0, p_1 e p_2 são fórmulas do CP;
- ii. Por i. e pela regra (F_3), $(\neg p_0)$ é uma fórmula do CP;
- iii. Por i. e pela regra (F_4), $(p_1 \wedge p_2)$ é uma fórmula do CP;
- iv. Por ii., iii. e pela regra (F_6), $((\neg p_0) \rightarrow (p_1 \wedge p_2))$ é uma fórmula do CP.

[2] A palavra $((p_0 \vee (\neg \perp)) \leftrightarrow (p_1 \rightarrow p_0))$ é uma fórmula do Cálculo Proposicional, pois:

- i. Pela regra (F_1), \perp é uma fórmula do CP;
- ii. Pela regra (F_2), as variáveis proposicionais p_0 e p_1 são fórmulas do CP;
- iii. Por i. e pela regra (F_3), $(\neg \perp)$ é uma fórmula do CP;
- iv. Por ii., por iii. e pela regra (F_5), $(p_1 \vee (\neg \perp))$ é uma fórmula do CP;
- v. Por ii. e pela regra (F_6), $(p_1 \rightarrow p_0)$ é uma fórmula do CP;
- vi. Por iv., v. e pela regra (F_7), $((p_1 \vee (\neg \perp)) \leftrightarrow (p_1 \rightarrow p_0))$ é uma fórmula do CP.

[3] A palavra (p_0) não é uma fórmula do Cálculo Proposicional, uma vez que não pode ser obtida a partir de \perp ou de variáveis proposicionais por aplicação de um número finito das operações descritas em (F_3) – (F_7). De facto, não pode haver ocorrências de parêntesis numa fórmula do Cálculo Proposicional sem haver a ocorrência de pelo menos um dos conetivos $\neg, \wedge, \vee, \rightarrow$ ou \leftrightarrow .

[4] A palavra $\neg p_0 \wedge$ não é uma fórmula do Cálculo Proposicional, uma vez que não pode ser obtida a partir de \perp ou de variáveis proposicionais por aplicação de um número finito das operações descritas em (F_3) – (F_7). Com efeito, não é possível obter uma palavra, por aplicação das referidas operações, cuja última letra seja \wedge .

[5] A palavra $(p_0 \vee p_1)$ não é uma fórmula do Cálculo Proposicional, uma vez que não pode ser obtida a partir de \perp ou de variáveis proposicionais por aplicação de um número finito das operações descritas em (F3) – (F7). Efetivamente, o número de ocorrências de parêntesis numa fórmula do Cálculo Proposicional é sempre par.

Para que uma palavra seja considerada uma fórmula do Cálculo Proposicional, é necessário que os parêntesis ocorram de acordo com as regras que definem o conjunto de fórmulas.

No entanto, os parêntesis extremos e os parêntesis à volta de negações são muitas vezes omitidos, por simplificação de escrita. Por exemplo, a palavra

$$(p_5 \wedge \neg p_0) \vee \perp$$

será utilizada como uma representação da fórmula

$$((p_5 \wedge (\neg p_0)) \vee \perp).$$

Por abuso de linguagem, chamaremos fórmulas a tais representações de fórmulas.

[Exemplo]

A fórmula $((\neg p_0) \vee p_1) \leftrightarrow (p_2 \wedge (\neg p_0))$ pode ser representada pela palavra $(\neg p_0 \vee p_1) \leftrightarrow (p_2 \wedge \neg p_0)$.

A palavra $\neg(p_0 \vee \neg p_1)$ é uma representação da fórmula $(\neg(p_0 \vee (\neg p_1)))$, ao passo que $\neg p_0 \vee \neg p_1$ não o é.

A fórmula $(p_0 \wedge (p_1 \vee p_2))$ pode ser representada por $p_0 \wedge (p_1 \vee p_2)$ mas não pode ser representada por $p_0 \wedge p_1 \vee p_2$.

1.2.2 Semântica

A sintaxe do Cálculo Proposicional não nos permite atribuir qualquer significado às fórmulas. De facto, uma fórmula, por si só, não tem qualquer significado – este depende da interpretação associada aos símbolos.

[Exemplo]

Se p_0 representar a afirmação “ $2 \times 7 = 14$ ” e p_1 representar a afirmação “ $1 + 2 \times 7 = 15$ ”, então a fórmula $(p_0 \rightarrow p_1)$ representa a afirmação “Se $2 \times 7 = 14$, então $1 + 2 \times 7 = 15$ ”, que é verdadeira.

Por outro lado, se p_0 representar a afirmação “ $2 \times 7 = 14$ ” e p_1 representar a afirmação “ $1 + 2 \times 7 = 16$ ”, então a fórmula $(p_0 \rightarrow p_1)$ representa a afirmação “Se $2 \times 7 = 14$, então $1 + 2 \times 7 = 16$ ”, que é falsa.

A semântica do Cálculo Proposicional consiste na atribuição de **valores de verdade** às suas fórmulas.

Em lógica clássica, são considerados dois valores de verdade.

[Definição 1.3] Os valores lógicos (ou valores de verdade) do Cálculo Proposicional são **verdadeiro** (**V** ou **1**) e **falso** (**F** ou **0**).

Interessa-nos considerar frases declarativas sobre as quais se pode decidir acerca do seu valor lógico.

[Definição 1.4] Uma **proposição** é uma frase declarativa sobre a qual é possível dizer objetivamente se é verdadeira ou falsa (ainda que possamos não ser capazes de, no momento atual, determinar o seu valor lógico).

A afirmação “5 é um número par” é uma proposição (no caso falsa) já que o seu valor lógico não depende do sujeito que o atribui. O mesmo acontece com a afirmação “ $x^2 = -1$ não tem soluções reais”, sendo esta proposição verdadeira. A afirmação “Existe vida em Marte” é uma proposição. Esta afirmação será verdadeira ou falsa (mas não ambas as coisas), apesar de não sabermos o seu valor lógico. Outras afirmações existem, por seu turno, que por falta de objetividade na atribuição do valor lógico, não podem ser consideradas proposições. A título de exemplo, a afirmação “Os alunos da UM são os melhores alunos universitários do país”. A não objetividade da afirmação parece óbvia. Ainda outro exemplo, “Esta proposição é falsa”.

Existem, ainda, outras afirmações de índole matemática às quais não é possível aferir o valor lógico. Por exemplo, “ $x \geq 6$ ” tem o seu valor lógico dependente do valor que se atribui a x , pelo que não é uma proposição.

[Exemplo]

Consideremos as seguintes frases:

[1] Lisboa é a capital de Portugal.

[2] $2 + 3 = 6$

[3] Quando é que vamos almoçar?

[4] Toma um café.

[5] $2+x=6$

[6] Todo o número maior ou igual a 4 pode ser escrito como a soma de dois números primos.

[7] 2 é um número par.

As frases 1, 2, 6 e 7 são proposições: as afirmações 1 e 7 são verdadeiras, enquanto que a afirmação 2 é falsa.

A afirmação 6 é conhecida como a *Conjetura de Goldbach* – até ao momento, não existe uma prova da sua veracidade ou da sua falsidade, mas será possível associar-lhe um e um só dos dois valores lógicos.

As restantes frases não são proposições: as frases 3 e 4 não são do tipo declarativo e, portanto, não é possível associar-lhes um dos valores lógicos; a frase 5 não é nem verdadeira nem falsa, visto que o valor de x é desconhecido.

[Definição 1.5] Uma proposição diz-se uma **proposição simples** se se tratar de uma frase declarativa simples. Diz-se uma **proposição composta** se for uma frase declarativa composta.

A veracidade de uma frase simples pode depender do contexto em que esta é considerada. Por exemplo, a afirmação “Este livro tem uma capa vermelha.” pode ser verdadeira ou falsa, dependendo do livro em causa.

Também a decisão sobre o valor lógico de uma frase composta pode depender do contexto em que se insere. No entanto, para saber se uma frase composta é verdadeira ou falsa, basta saber o que acontece com as frases simples que a compõem. A afirmação “Este livro tem uma capa vermelha e está escrito em português.” é verdadeira para alguns livros e falsa para outros. Porém, é verdadeira sempre que ambas as frases simples que a compõem forem verdadeiras.

[Exemplo]

Consideremos as seguintes proposições:

[1] 2 é um número par.

[2] Todo o número primo é ímpar.

[3] 2 é um número par e todo o número primo é ímpar.

A proposição 1 é uma proposição simples que assume o valor lógico verdadeiro, enquanto que a proposição 2 é uma proposição simples que assume o valor lógico falso. A proposição 3 é composta: obtém-se a partir da conjunção de duas proposições simples. Como uma das proposições simples que a compõem é falsa, assume também o valor lógico falso.

No Cálculo Proposicional, não se pretende determinar se uma frase simples é ou não verdadeira. O objetivo é estudar a veracidade das proposições compostas a partir da veracidade ou falsidade das frases que as compõem e do significado dos conetivos.

Estudaremos de seguida o significado associado a cada um dos conetivos proposicionais referidos anteriormente. Esse mesmo significado pode ser expresso de forma clara através de tabelas designadas por **tabelas de verdade**.

Por Definição, a fórmula \perp toma sempre o valor lógico 0.

Dada uma proposição arbitrária φ , a sua negação tem um valor lógico contrário ao de φ . A relação entre o valor lógico de φ e o valor lógico de $\neg\varphi$ pode ser representada através da seguinte tabela de verdade:

φ	$\neg\varphi$
1	0
0	1

[Exemplo]

A proposição “Todo o número primo é ímpar.” é falsa. A sua negação, “Nem todo o número primo é ímpar.”, é verdadeira: basta considerar o número primo 2.

A proposição “24 é divisível por 8.” é verdadeira. A sua negação, “24 não é divisível por 8.” é falsa, uma vez que $24 = 8 \times 3$.

Dadas duas proposições φ e ψ , a conjunção de φ e ψ é verdadeira somente se ambas as proposições que a compõem são verdadeiras. A tabela de verdade associada ao conetivo \wedge é a seguinte:

φ	ψ	$\varphi \wedge \psi$
1	1	1
1	0	0
0	1	0
0	0	0

[Exemplo]

As proposições “24 é divisível por 8.” e “56 é divisível por 8.” são verdadeiras. Por outro lado, a proposição “28 é divisível por 8.” é falsa.

A proposição “24 e 56 são divisíveis por 8.”, que resulta da conjunção das duas primeiras proposições atrás referidas, é verdadeira. A proposição “28 e 56 são divisíveis por 8.” é falsa.

Dadas duas proposições φ e ψ , a disjunção de φ e ψ é verdadeira se pelo menos umas das proposições que a compõem é verdadeira. O significado do conetivo \vee é dado pela tabela seguinte:

φ	ψ	$\varphi \vee \psi$
1	1	1
1	0	1
0	1	1
0	0	0

[Exemplo]

A proposição “24 não é divisível por 8 ou 5 não é um número primo.” é falsa pois é a disjunção de duas proposições falsas. A proposição “24 não é divisível por 8 ou 100 é divisível por 4.” é verdadeira, pois uma das proposições que a compõem é verdadeira.

Dadas duas proposições φ e ψ , $\varphi \rightarrow \psi$ é verdadeira se ψ é verdadeira sempre que φ é verdadeira. O significado do conetivo \rightarrow é dado pela tabela seguinte:

φ	ψ	$\varphi \rightarrow \psi$
1	1	1
1	0	0
0	1	1
0	0	1

[Exemplo]

Consideremos a seguinte afirmação “Se o João tiver 12 valores no teste, então o João passa à disciplina.”

Note-se que esta afirmação será falsa se o João tiver 12 valores no teste e não passar à disciplina. Por outro lado, será claramente verdadeira se o João tiver 12 valores no teste e passar à disciplina. A afirmação não descreve o que acontece caso o João não tire 12 valores no teste. Sendo assim, caso o João não tire 12 valores no teste, a afirmação é verdadeira quer o João passe à disciplina quer não passe. Resumindo, a afirmação é falsa se o antecedente da implicação é verdadeiro e o consequente falso, e só nesse caso.

Dadas duas proposições φ e ψ , $\varphi \leftrightarrow \psi$ é verdadeira se ψ e φ são simultaneamente verdadeiras ou simultaneamente falsas. O significado do conetivo \leftrightarrow é dado pela tabela seguinte:

φ	ψ	$\varphi \leftrightarrow \psi$
1	1	1
1	0	0
0	1	0
0	0	1

[Exemplo]

Consideremos as seguintes proposições:

[1] $1 + 3 = 4$ é equivalente a $4 = 1 + 3$.

[2] $1 + 1 = 1$ se e só se chover canivetes.

[3] 10 é múltiplo de 5 se e só se 8 é múltiplo de 5.

A proposição 3 é falsa, ao passo que as restantes são verdadeiras.

Conhecidos os valores lógicos das variáveis proposicionais que ocorrem numa fórmula, esta tem associado um e um só **valor lógico**. Na análise de qual será o valor lógico de uma fórmula, relacionando-o com os valores lógicos das variáveis que nela ocorrem, é útil o recurso a tabelas de verdade.

[Exemplo]

Estudemos o valor lógico da fórmula $\varphi = \neg p_0 \wedge (p_1 \vee p_0)$.

Nesta fórmula ocorrem duas variáveis proposicionais, p_0 e p_1 , pelo que se torna necessário considerar todas as combinações possíveis dos valores lógicos de p_0 e p_1 .

Como cada variável pode assumir um de dois valores lógicos (0 ou 1), existem 2^2 combinações possíveis. Logo, a tabela de verdade terá 4 linhas. Introduzimos uma coluna para cada variável proposicional, uma coluna para φ e colunas (auxiliares) para cada uma das restantes subfórmulas de φ .

p_0	p_1	$\neg p_0$	$p_1 \vee p_0$	$\neg p_0 \wedge (p_1 \vee p_0)$
1	1			
1	0			
0	1			
0	0			

Para cada caso, determinamos primeiro o valor lógico de $\neg p_0$ e de $p_1 \vee p_0$, para podermos, depois, determinar o valor lógico de $\neg p_0 \wedge (p_1 \vee p_0)$.

p_0	p_1	$\neg p_0$	$p_1 \vee p_0$	$\neg p_0 \wedge (p_1 \vee p_0)$
1	1	0	1	
1	0	0	1	
0	1	1	1	
0	0	1	0	

Da análise da seguinte tabela de verdade

p_0	p_1	$\neg p_0$	$p_1 \vee p_0$	$\neg p_0 \wedge (p_1 \vee p_0)$
1	1	0	1	0
1	0	0	1	0
0	1	1	1	1
0	0	1	0	0

podemos concluir que a fórmula φ é verdadeira apenas quando p_0 é falsa e p_1 é verdadeira.

[Exemplo]

Estudemos, agora, o valor lógico da fórmula $\psi = \neg(p_0 \vee p_1) \rightarrow p_2$.

Nesta fórmula ocorrem três variáveis proposicionais distintas, p_0 , p_1 e p_2 , pelo que existem 2^3 combinações dos valores lógicos de p_0 , p_1 e p_2 . Logo, a tabela de verdade para a fórmula ψ terá 8 linhas:

p_0	p_1	p_2	$p_0 \vee p_1$	$\neg(p_0 \vee p_1)$	$\neg(p_0 \vee p_1) \rightarrow p_2$
1	1	1	1	0	1
1	1	0	1	0	1
1	0	1	1	0	1
1	0	0	1	0	1
0	1	1	1	0	1
0	1	0	1	0	1
0	0	1	0	1	1
0	0	0	0	1	0

Analisando a tabela, podemos concluir que a fórmula ψ é falsa apenas quando as três variáveis proposicionais p_0 , p_1 e p_2 são todas falsas.

[Observação] Se φ é uma fórmula onde ocorrem n variáveis proposicionais distintas, então existem 2^n combinações possíveis para os valores lógicos dessas variáveis proposicionais. Assim, uma tabela de verdade de φ terá 2^n linhas.

Existem fórmulas que assumem sempre o valor lógico verdadeiro qualquer que seja a combinação dos valores lógicos das variáveis proposicionais que nelas ocorrem.

[Definição 1.6] Uma **tautologia** é uma fórmula que assume sempre o valor lógico verdadeiro, independentemente dos valores lógicos das variáveis proposicionais que a compõem.

[Exemplo]

Para cada $n \in \mathbb{N}_0$, as fórmulas $p_n \vee \neg p_n$ e $p_n \rightarrow p_n$ são tautologias.

p_n	$\neg p_n$	$p_n \vee \neg p_n$	p_n	$p_n \rightarrow p_n$
1	0	1	1	1
0	1	1	0	1

No resultado que se segue, listam-se tautologias que são utilizadas com frequência.

[Proposição 1.7] Dadas as fórmulas proposicionais φ , ψ e σ , as seguintes fórmulas são tautologias:

[Modus Ponens] $(\varphi \wedge (\varphi \rightarrow \psi)) \rightarrow \psi$

[Modus Tollens] $((\varphi \rightarrow \psi) \wedge \neg \psi) \rightarrow \neg \varphi$

[transitividade] $((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \sigma)) \rightarrow (\varphi \rightarrow \sigma)$

demonstração: Verifiquemos se a fórmula que expressa a transitividade é uma tautologia.

Construindo a tabela de verdade de $\tau : ((\varphi \rightarrow \psi) \wedge (\psi \rightarrow \sigma)) \rightarrow (\varphi \rightarrow \sigma)$, podemos concluir que esta fórmula é uma tautologia se o seu valor lógico for sempre verdadeiro.

φ	ψ	σ	$\varphi \rightarrow \psi$	$\psi \rightarrow \sigma$	$(\varphi \rightarrow \psi) \wedge (\psi \rightarrow \sigma)$	$\varphi \rightarrow \sigma$	τ
1	1	1	1	1	1	1	1
1	1	0	1	0	0	0	1
1	0	1	0	1	0	1	1
1	0	0	0	1	0	0	1
0	1	1	1	1	1	1	1
0	1	0	1	0	0	1	1
0	0	1	1	1	1	1	1
0	0	0	1	1	1	1	1

De modo análogo, verifica-se que as outras duas fórmulas que expressam o Modus Tollens e o Modus Ponens são tautologias (exercício). ■

A negação de uma tautologia é uma fórmula que assume sempre o valor lógico falso.

[Definição 1.8] Uma **contradição** é uma fórmula que assume sempre o valor lógico falso, independentemente dos valores lógicos das variáveis proposicionais que a compõem.

[Exemplo]

As fórmulas $p_n \wedge \neg p_n$ e $p_n \leftrightarrow \neg p_n$ são contradições para todo o $n \in \mathbb{N}_0$.

p_n	$\neg p_n$	$p_n \wedge \neg p_n$
1	0	0
0	1	0

p_n	$\neg p_n$	$p_n \leftrightarrow \neg p_n$
1	0	0
0	1	0

[Observações]

(1) Se uma fórmula não é uma tautologia, isso não significa que seja uma contradição. Há, evidentemente, fórmulas que não são nem tautologias nem contradições.

(2) Se φ é uma tautologia (respetivamente, contradição), então $\neg\varphi$ é uma contradição (respetivamente, tautologia).

Existem fórmulas que, embora distintas, assumem o mesmo valor lógico para cada uma das combinações possíveis dos valores lógicos das variáveis proposicionais que nelas ocorrem. Se φ e ψ forem duas fórmulas nessas condições, facilmente concluímos que $\varphi \leftrightarrow \psi$ é uma tautologia.

[Definição 1.9] Sejam φ e ψ duas fórmulas proposicionais. Dizemos que φ e ψ são **logicamente equivalentes** se $\varphi \leftrightarrow \psi$ é uma tautologia. Neste caso, escrevemos $\varphi \Leftrightarrow \psi$.

[Exemplo]

As fórmulas $\varphi : (p_0 \wedge (p_1 \vee p_0)) \rightarrow \neg p_1$ e $\psi : \neg(p_0 \wedge p_1)$ são logicamente equivalentes, pois

$$\varphi \leftrightarrow \psi : ((p_0 \wedge (p_1 \vee p_0)) \rightarrow \neg p_1) \leftrightarrow (\neg(p_0 \wedge p_1))$$

é uma tautologia.

p_0	p_1	$p_1 \vee p_0$	$p_0 \wedge (p_1 \vee p_0)$	$\neg p_1$	φ	$p_0 \wedge p_1$	ψ	$\varphi \leftrightarrow \psi$
1	1	1	1	0	0	1	0	1
1	0	1	1	1	1	0	1	1
0	1	1	0	0	1	0	1	1
0	0	0	0	1	1	0	1	1

Em seguida, listamos algumas das equivalências lógicas mais conhecidas e frequentemente utilizadas.

[Proposição 1.10] Dadas fórmulas proposicionais φ , ψ e σ , são válidas as seguintes equivalências lógicas:

[associatividade]

$$((\varphi \wedge \psi) \wedge \sigma) \Leftrightarrow (\varphi \wedge (\psi \wedge \sigma))$$

$$((\varphi \vee \psi) \vee \sigma) \Leftrightarrow (\varphi \vee (\psi \vee \sigma))$$

[leis de De Morgan]

$$\neg(\varphi \wedge \psi) \Leftrightarrow (\neg\varphi \vee \neg\psi)$$

$$\neg(\varphi \vee \psi) \Leftrightarrow (\neg\varphi \wedge \neg\psi)$$

[comutatividade]

$$((\varphi \wedge \psi) \Leftrightarrow (\psi \wedge \varphi))$$

$$((\varphi \vee \psi) \Leftrightarrow (\psi \vee \varphi))$$

[distributividade]

$$((\varphi \wedge (\psi \vee \sigma)) \Leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \sigma))$$

$$((\varphi \vee (\psi \wedge \sigma)) \Leftrightarrow ((\varphi \vee \psi) \wedge (\varphi \vee \sigma))$$

[idempotência]

$$(\varphi \wedge \varphi) \Leftrightarrow \varphi$$

$$(\varphi \vee \varphi) \Leftrightarrow \varphi$$

[dupla negação]

$$\neg(\neg\varphi) \Leftrightarrow \varphi$$

[elemento neutro]

$$((\varphi \wedge (\psi \vee \neg\psi)) \Leftrightarrow \varphi$$

$$((\varphi \vee (\psi \wedge \neg\psi)) \Leftrightarrow \varphi$$

[elemento absorvente]

$$((\varphi \wedge (\psi \wedge \neg\psi)) \Leftrightarrow (\psi \wedge \neg\psi)$$

$$((\varphi \vee (\psi \vee \neg\psi)) \Leftrightarrow (\psi \vee \neg\psi)$$

[lei do contrarrecíproco]

$$(\varphi \rightarrow \psi) \Leftrightarrow (\neg\psi \rightarrow \neg\varphi)$$

$$(\varphi \leftrightarrow \psi) \Leftrightarrow (\varphi \rightarrow \psi) \wedge (\psi \rightarrow \varphi)$$

$$(\varphi \rightarrow \psi) \Leftrightarrow (\neg\varphi \vee \psi)$$

demonstração: Começamos por mostrar a equivalência lógica da dupla negação.

Construindo a tabela de verdade de $\neg(\neg\varphi) \leftrightarrow \varphi$, concluímos que esta fórmula é uma tautologia:

φ	$\neg\varphi$	$\neg(\neg\varphi)$	$\neg(\neg\varphi) \leftrightarrow \varphi$
1	0	1	1
0	1	0	1

Logo, as fórmulas $\neg(\neg\varphi)$ e φ são logicamente equivalentes.

Verifiquemos, agora, a equivalência lógica

$$((\varphi \wedge (\psi \vee \sigma)) \Leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \sigma))).$$

As restantes provas ficam como exercício.

À semelhança do que foi feito no caso da dupla negação, construindo a tabela de verdade de $\tau : ((\varphi \wedge (\psi \vee \sigma)) \Leftrightarrow ((\varphi \wedge \psi) \vee (\varphi \wedge \sigma)))$, concluímos que esta fórmula é uma tautologia:

φ	ψ	σ	$\psi \vee \sigma$	$\varphi \wedge (\psi \vee \sigma)$	$\varphi \wedge \psi$	$\varphi \wedge \sigma$	$(\varphi \wedge \psi) \vee (\varphi \wedge \sigma)$	τ
1	1	1	1	1	1	1	1	1
1	1	0	1	1	1	0	1	1
1	0	1	1	1	0	1	1	1
1	0	0	0	0	0	0	0	1
0	1	1	1	0	0	0	0	1
0	1	0	1	0	0	0	0	1
0	0	1	1	0	0	0	0	1
0	0	0	0	0	0	0	0	1

■

[Exemplo]

Usando uma sequência de equivalências lógicas, podemos mostrar que a fórmula

$$(p_0 \wedge p_1) \vee (p_0 \wedge (\neg p_1)),$$

é logicamente equivalente à fórmula p_0 .

De facto,

$$\begin{aligned} (p_0 \wedge p_1) \vee (p_0 \wedge (\neg p_1)) &\Leftrightarrow p_0 \wedge (p_1 \vee \neg p_1) && \text{[distributividade]} \\ &\Leftrightarrow p_0 && \text{[elemento neutro]} \end{aligned}$$

Poderíamos, também, mostrar que a fórmula $(p_0 \wedge p_1) \vee (p_0 \wedge (\neg p_1))$ é logicamente equivalente a p_0 provando que a fórmula $((p_0 \wedge p_1) \vee (p_0 \wedge (\neg p_1))) \Leftrightarrow p_0$ é uma tautologia.

[Exemplo]

Usando uma sequência de equivalências lógicas, podemos provar que as fórmulas $p_0 \rightarrow (p_1 \rightarrow p_2)$ e $\neg(\neg p_2 \rightarrow \neg p_1) \rightarrow \neg p_0$ são logicamente equivalentes.

Pela lei do contrarrecíproco,

$$(p_1 \rightarrow p_2) \Leftrightarrow (\neg p_2 \rightarrow \neg p_1),$$

pelo que

$$(p_0 \rightarrow (p_1 \rightarrow p_2)) \Leftrightarrow (p_0 \rightarrow (\neg p_2 \rightarrow \neg p_1)).$$

De novo pela lei do contrarrecíproco, temos

$$(p_0 \rightarrow (\neg p_2 \rightarrow \neg p_1)) \Leftrightarrow (\neg(\neg p_2 \rightarrow \neg p_1) \rightarrow \neg p_0).$$

Assim,

$$(p_0 \rightarrow (p_1 \rightarrow p_2)) \Leftrightarrow (\neg(\neg p_2 \rightarrow \neg p_1) \rightarrow \neg p_0).$$

1.3 Cálculo de Predicados Clássico

Na secção anterior, referimos que frases como “ x é um inteiro par” ou “ $x + y = 2$ ” não são proposições, visto que os seus valores lógicos dependem dos valores de x e de y .

No entanto, é frequente encontrarmos, no estudo de qualquer teoria matemática, frases que fazem referência a objetos genéricos representados por letras, designadas por **variáveis**.

Frases como esta são objeto de estudo de um ramo da lógica denominado Cálculo de Predicados.

Nesta Unidade Curricular, não pretendemos aprofundar o estudo de Cálculo de Predicados, mas iremos estudar algumas noções elementares que permitam a familiarização com o simbolismo, o significado, o uso e a negação de frases quantificadas.

Em frases que envolvam variáveis, está implícito um domínio de discurso, designado por **universo** ou **domínio de variação** das variáveis.

[Exemplo]

Na frase “ x é um inteiro par”, a variável x refere-se a um inteiro, pelo que o universo de x é o conjunto \mathbb{Z} .

A frase “ x é um inteiro par” não é uma proposição. No entanto, se substituirmos x por valores do seu universo, obtemos frases às quais já é possível associar um valor de verdade. Por exemplo, “2 é um inteiro par” e “3 é um inteiro par” são proposições que assumem o valor lógico verdadeiro e falso, respetivamente.

[Definição 1.11] Um **predicado nas variáveis** x_1, \dots, x_n , com $n \in \mathbb{N}$, é uma frase declarativa que faz referência às variáveis x_1, \dots, x_n cujo valor lógico depende da substituição destas variáveis por valores do seu domínio de variação, tornando-se numa proposição sempre que as variáveis são substituídas por valores do seu universo.

Representamos um predicado nas variáveis x_1, \dots, x_n por uma letra minúscula p, q, r, \dots (eventualmente com índices) seguida das variáveis que ocorrem nesse predicado colocadas entre parêntesis e separadas por vírgulas.

[Exemplo]

Os predicados “ x é um inteiro par” e “ x é maior do que y ” podem ser representados, respetivamente, por $p(x)$ e por $q(x, y)$.

Dado um predicado $p(x_1, \dots, x_n)$, com $n \in \mathbb{N}$, se, para cada $i \in \{1, \dots, n\}$, a_i é um valor do domínio de variação de x_i , então representamos por $p(a_1, \dots, a_n)$ a substituição das variáveis de p por esses valores concretos.

[Exemplo]

Considerando os predicados do exemplo anterior, $p(8)$ representa a proposição “8 é um inteiro par” e $q(\sqrt{2}, 3)$ representa a proposição “ $\sqrt{2}$ é maior do que 3”.

Os conetivos lógicos que definimos na sintaxe do Cálculo Proposicional Clássico estendem-se ao Cálculo de Predicados de um modo natural.

Assim, se $p(x_1, \dots, x_n)$ e $q(x_1, \dots, x_n)$ são predicados nas variáveis x_1, \dots, x_n , então

$$\begin{aligned} &(\neg p(x_1, \dots, x_n)), \quad (p(x_1, \dots, x_n) \wedge q(x_1, \dots, x_n)), \\ &(p(x_1, \dots, x_n) \vee q(x_1, \dots, x_n)), \quad (p(x_1, \dots, x_n) \rightarrow q(x_1, \dots, x_n)) \\ &\text{e} \quad (p(x_1, \dots, x_n) \leftrightarrow q(x_1, \dots, x_n)) \end{aligned}$$

são também predicados nas variáveis x_1, \dots, x_n .

[Exemplo]

Sejam $p(x)$ o predicado “ x é um inteiro par” e $q(x)$ o predicado “ x é um número primo”. Então, $p(x) \wedge q(x)$ representa o predicado “ x é um inteiro par e é um número primo”.

A substituição das variáveis de um predicado por valores concretos dos seus domínios de variação não é a única forma de obter uma proposição a partir de um predicado. Também o podemos fazer recorrendo aos chamados **quantificadores**.

[Definição 1.12] Sejam $n \in \mathbb{N}$ e $i \in \{1, \dots, n\}$. Se $p(x_1, \dots, x_n)$ é um predicado nas variáveis x_1, \dots, x_n , a frases tais como “Para todo o x_i , $p(x_1, \dots, x_i, \dots, x_n)$.”, “Qualquer que seja o x_i , $p(x_1, \dots, x_i, \dots, x_n)$.”, “Para cada x_i , $p(x_1, \dots, x_i, \dots, x_n)$.”, dá-se a designação de **quantificação universal**. Estas frases podem ser representadas por $\forall_{x_i} p(x_1, \dots, x_i, \dots, x_n)$.

Ao símbolo \forall chamamos **quantificador universal** e é usual associarmos-lhe uma das seguintes leituras: “todo”, “para todo”, “qualquer que seja” ou “para cada”.

Se $p(x)$ é um predicado na variável x , a frase representada por $\forall_x p(x)$ é uma proposição.

A proposição $\forall_x p(x)$ é verdadeira se $p(a)$ for verdadeira para **todo** o elemento a do domínio de variação de x , também designado **universo de quantificação de x** .

[Exemplo]

Se $p(x)$ representar o predicado “ $x^2 \geq 0$ ” e se o universo de quantificação de x for o conjunto dos reais, a proposição $\forall_x p(x)$ é verdadeira, uma vez que a afirmação em causa é verdadeira para qualquer real.

Se existir (pelo menos) um elemento b do domínio de variação de x para o qual $p(b)$ é uma proposição falsa, a proposição $\forall_x p(x)$ é falsa.

[Exemplo]

Se $q(x)$ representar o predicado $x^2 > 0$ e se o universo de quantificação de x for o conjunto dos reais, a proposição $\forall_x q(x)$ é falsa, pois 0 é um número real e $q(0)$ é falsa.

[Definição 1.13] Sejam $n \in \mathbb{N}$ e $i \in \{1, \dots, n\}$. Se $p(x_1, \dots, x_n)$ é um predicado nas variáveis x_1, \dots, x_n , frases tais como “Existe um x_i tal que $p(x_1, \dots, x_i, \dots, x_n)$.”, “Para algum x_i , $p(x_1, \dots, x_i, \dots, x_n)$.” são designadas de **quantificação existencial**.

Estas frases podem ser representadas por $\exists_{x_i} p(x_1, \dots, x_i, \dots, x_n)$. Ao símbolo \exists chamamos **quantificador existencial** e é usual associarmos-lhe uma das seguintes leituras: “existe” ou “para algum”.

Se $p(x)$ é um predicado na variável x , a frase representada por $\exists_x p(x)$ é uma proposição.

A proposição $\exists_x p(x)$ é verdadeira se $p(a)$ for verdadeira para **algum** elemento a do universo de quantificação de x .

Por outro lado, se não existir qualquer elemento b do universo de quantificação de x para o qual $p(b)$ seja verdadeira, a proposição $\exists_x p(x)$ é falsa.

[Exemplo]

Se $p(x)$ representar o predicado “ $x + 3 = 2$ ” e se o universo de quantificação de x for o conjunto dos números inteiros, a proposição $\exists_x p(x)$ é verdadeira, pois $-1 \in \mathbb{Z}$ e $p(-1)$ é verdadeira.

Por outro lado, se o universo de quantificação de x for o conjunto dos números naturais, a proposição $\exists_x p(x)$ é falsa, uma vez que a equação não tem solução em \mathbb{N} .

Se o universo de uma dada quantificação for um certo conjunto U , podemos escrever $\forall_{x \in U} p(x)$ e $\exists_{x \in U} p(x)$, em vez de $\forall_x p(x)$ e $\exists_x p(x)$, respetivamente.

[Exemplo]

A frase “Existe um natural x tal que $x + 3 = 2$ ” pode ser representada por

$$\exists_{x \in \mathbb{N}} x + 3 = 2.$$

Relativamente ao predicado $p(x) : x + 3 = 2$, prova-se que o número inteiro -1 é, de facto, o único inteiro a tal que $p(a)$ é uma proposição verdadeira.

Se $p(x)$ é um predicado na variável x , a existência de um único objeto que satisfaça o predicado $p(x)$ pode ser representada pela expressão $\exists_x^1 p(x)$, à qual é usual associar uma das leituras “Existe um e um só x tal que $p(x)$ ” ou “Existe um único x tal que $p(x)$ ”.

[Exemplo]

A proposição $\exists_{x \in \mathbb{Z}}^1 x + 3 = 2$ é verdadeira, ao passo que $\exists_{x \in \mathbb{Z}}^1 x^2 - 1 = 0$ é falsa (tanto 1 como -1 satisfazem o predicado $x^2 - 1 = 0$, contradizendo a unicidade de um objeto que o satisfaça).

Os quantificadores universal e existencial podem ser combinados para quantificar uma mesma condição.

[Exemplo]

Sejam $p(x, y)$ o predicado $(x + y)^2 = x^2 + 2xy + y^2$ e $q(x, y)$ o predicado $x + y = 0$.

Dados dois números reais quaisquer a e b , sabemos que $p(a, b)$ é verdadeira. Logo, a proposição $\forall_{x \in \mathbb{R}} \forall_{y \in \mathbb{R}} p(x, y)$ é verdadeira.

Todo o número inteiro admite um simétrico em \mathbb{Z} , pelo que a proposição $\forall_{x \in \mathbb{Z}} \exists_{y \in \mathbb{Z}} q(x, y)$ é verdadeira.

No entanto, a proposição $\forall_{x \in \mathbb{N}_0} \exists_{y \in \mathbb{N}_0} q(x, y)$ é falsa.

[Exemplo]

Consideremos as seguintes proposições.

- [a] A equação $x^3 = 27$ tem solução no conjunto dos números naturais.
- [b] Todo o número real admite um inverso para a multiplicação.
- [c] Todo o inteiro maior ou igual a 4 pode ser escrito como a soma de dois números primos.
- [d] No conjunto dos números reais, existe um elemento absorvente para a multiplicação e este elemento é único.

Todas são quantificações e podemos, sem grande dificuldade, exprimi-las em linguagem formal:

$$[a] \exists_{x \in \mathbb{N}} x^3 = 27$$

$$[b] \forall_{x \in \mathbb{R}} \exists_{y \in \mathbb{R}} xy = 1$$

$$[c] \forall_{n \in \mathbb{Z}} (n \geq 4 \rightarrow (\exists_{m,p \in \mathbb{Z} \setminus \{1\}} (n = m + p \wedge \forall_{k \in \mathbb{N}} ((k|m \rightarrow (k = 1 \vee k = m)) \wedge (k|p \rightarrow (k = 1 \vee k = p))))))$$

$$[d] \exists_{y \in \mathbb{R}}^1 \forall_{x \in \mathbb{R}} xy = yx = y$$

Quando temos um predicado em duas ou mais variáveis, a valoração da proposição obtida pela quantificação de todas as variáveis pode depender da ordem dessas quantificações.

[Exemplo]

Consideremos o predicado $x + y = 5$.

A proposição $\forall_{x \in \mathbb{Z}} \exists_{y \in \mathbb{Z}} x + y = 5$ é verdadeira. De facto, dado $x \in \mathbb{Z}$, temos que $x + y = 5$ para $y = 5 - x$, que é, claramente, um inteiro.

A proposição $\exists_{y \in \mathbb{Z}} \forall_{x \in \mathbb{Z}} x + y = 5$ é falsa, já que afirma que existe um inteiro y tal que $x + y = 5$ para todo o $x \in \mathbb{Z}$ (portanto, um mesmo valor de y para todos os valores de x). Ora, para $x = 0$, tal y teria de ser 5, mas para $x = 1$, considerando $y = 5$, teríamos $x + y = 6 \neq 5$.

De notar que, quando as quantificações de todas as variáveis é feita com o mesmo quantificador, a ordem das quantificações não afeta a valoração da proposição e, como tal, é possível simplificar a escrita, usando apenas um quantificador.

[Exemplo]

A proposição (verdadeira) $\exists_{x \in \mathbb{Z}} \exists_{y \in \mathbb{Z}} x + y = 5$ pode ser escrita como $\exists_{x,y \in \mathbb{Z}} x + y = 5$.

A proposição (falsa) $\forall_{x \in \mathbb{Z}} \forall_{y \in \mathbb{Z}} x + y = 5$ pode ser escrita como $\forall_{x,y \in \mathbb{Z}} x + y = 5$.

Se a proposição $\exists_x p(x)$ é falsa, então não existe qualquer valor a do domínio de quantificação de x para o qual $p(a)$ seja verdadeira. Por outras palavras, $p(a)$ é falsa para todo o elemento a do domínio de quantificação de x . Equivalentemente, podemos afirmar que $\neg p(a)$ é verdadeira para todo o elemento a do domínio de quantificação de x , isto é, a proposição $\forall_x (\neg p(x))$ é verdadeira. Deste modo, provamos a seguinte proposição:

[Proposição 1.14] $\neg(\exists_x p(x))$ é logicamente equivalente a $\forall_x (\neg p(x))$.

De modo análogo, podemos concluir o resultado que se segue.

[Proposição 1.15] $\neg(\forall_x p(x))$ é logicamente equivalente a $\exists_x (\neg p(x))$.

[Exemplo]

Consideremos a proposição “1000000 é o maior número natural.

Usando linguagem simbólica, podemos reescrever a afirmação anterior como $\forall_{x \in \mathbb{N}} \ 1000000 > x$.

A negação da proposição é “1000000 não é o maior número natural”. Esta última proposição significa que existe pelo menos um natural que não é menor que 1000000.

Podemos, assim, reescrever a negação da proposição inicial como $\exists_{x \in \mathbb{N}} \ x \not\leq 1000000$ ou, equivalentemente, como $\exists_{x \in \mathbb{N}} \ x \geq 1000000$.

1.4 Métodos de Prova

[Definição 1.16] A prova (demonstração) de uma proposição matemática é um argumento logicamente válido (construído com base em princípios - regras e axiomas) que estabelece a veracidade da proposição.

[Exemplo]

Consideremos a proposição “ $2 = 1$ ” e a argumentação que se segue, que lhe conferiria o valor lógico verdadeiro.

Sejam $a, b \in \mathbb{Z}$.

$$\begin{aligned}
 a = b &\Rightarrow aa = ab \\
 &\Rightarrow a^2 = ab \\
 &\Rightarrow a^2 - b^2 = ab - b^2 \\
 &\Rightarrow (a + b)(a - b) = b(a - b) \\
 &\Rightarrow a + b = b \\
 &\Rightarrow b + b = b \\
 &\Rightarrow 2b = b \\
 &\Rightarrow 2 = 1
 \end{aligned}$$

Sabemos que a proposição “ $2 = 1$ ” é falsa, pelo que o argumento apresentado não pode ser válido. Uma vez que estamos a assumir que $a = b$, facilmente concluímos que $a - b = 0$, pelo que não podemos aplicar a lei do corte no quinto passo da argumentação. O argumento apresentado é, pois, incorreto.

A prova de uma proposição pode ser **direta** ou **indireta**.

Numa prova direta de uma proposição procura-se estabelecer a veracidade da mesma a partir de axiomas ou factos conhecidos e sem assumir pressupostos adicionais.

Porém, em certos casos, a prova direta não é simples e pode mesmo não ser possível. Nestas situações pode-se optar por um método de prova indireta. Por exemplo, pode-se provar a veracidade de uma proposição mostrando que esta não pode ser falsa.

1.4.1 Prova direta de uma conjunção

Na prova direta de $p \wedge q$, procura-se uma prova de p e uma prova de q .

De facto, sabemos que a proposição $p \wedge q$ é verdadeira se e só se ambas as proposições p e q são verdadeiras.

[Exemplo]

Consideremos a seguinte proposição: $x^2 + 2x + 2 = 0$ não tem soluções reais e as raízes do polinómio $x^2 - 1$ são -1 e 1.

Esta proposição é a conjunção das proposições

$$p: x^2 + 2x + 2 = 0 \text{ não tem soluções reais.}$$

e

$$q: \text{As raízes do polinómio } x^2 - 1 \text{ são -1 e 1.}$$

A prova direta da proposição dada consiste de uma prova da proposição p e de uma prova da proposição q :

demonstração: Usando a fórmula resolvente para equações polinomiais de 2.º grau, temos que

$$x^2 + 2x + 2 = 0 \Leftrightarrow x = \frac{-2 \pm \sqrt{-4}}{2}$$

Portanto, $x^2 + 2x + 2 = 0$ não tem soluções reais. Assim, p é uma proposição verdadeira.

Consideremos agora a equação $x^2 - 1 = 0$. Atendendo a que

$$x^2 - 1 = 0 \Leftrightarrow x^2 = 1 \Leftrightarrow x = -1 \vee x = 1,$$

podemos afirmar que as raízes do polinómio $x^2 - 1$ são -1 e 1 e, por conseguinte, que q é uma proposição verdadeira. ■

1.4.2 Prova direta de uma disjunção

Na prova direta de $p \vee q$ basta fazer prova de uma das proposições p ou q .

Recorde-se que a proposição $p \vee q$ é verdadeira se e só se pelo menos umas das proposições p ou q é verdadeira. Ao apresentar-se uma prova de p (respetivamente, q), fica provada a veracidade de $p \vee q$, sem ser necessário apresentar uma prova de q (respetivamente, p).

[Exemplo]

Consideremos a seguinte proposição: A soma de dois números naturais consecutivos é ímpar ou o seu produto é maior do que 3.

Esta proposição é a disjunção das proposições

p : A soma de dois números naturais consecutivos é ímpar.

e

q : O produto de dois números naturais consecutivos é maior do que 3.

A prova direta da proposição dada consiste de uma prova da proposição p ou de uma prova da proposição q . Neste caso, a proposição q é falsa em geral (note-se que 1 e 2 são naturais consecutivos cujo produto é inferior a 3), mas a prova da veracidade de p é suficiente para provar a veracidade de $p \vee q$:

demonstração: Sejam n e m dois números naturais consecutivos, com $n > m$. Então, $n = m + 1$, pelo que

$$n + m = (m + 1) + m = 2m + 1.$$

Assim, $n + m$ é um número ímpar. Logo, a soma de quaisquer dois números naturais consecutivos é ímpar e, portanto, a proposição é verdadeira. ■.

1.4.3 Prova direta de uma implicação

Para demonstrar diretamente uma afirmação do tipo $p \rightarrow q$, assume-se a veracidade de p e constrói-se uma prova de q .

Note-se que uma proposição $p \rightarrow q$ é verdadeira apenas nos casos em que p é falsa ou em que p e q são ambas verdadeiras. Assim, se p é uma proposição falsa, $p \rightarrow q$ é naturalmente verdadeira, independentemente do valor lógico de q . Logo, o único caso que é necessário analisar, para mostrar a veracidade de $p \rightarrow q$, é o caso em que p é verdadeira, sendo necessário provar, nesse caso, a veracidade de q .

[Exemplo]

Consideremos a proposição: Todo o inteiro ímpar se escreve como a diferença de dois quadrados perfeitos.

Esta proposição pode ser reescrita do seguinte modo: Se n é um inteiro ímpar, então n é a diferença de dois quadrados perfeitos. Assim, a proposição considerada é da forma $p \rightarrow q$, com

p : n é um inteiro ímpar.

e

q : n é a diferença de dois quadrados perfeitos.

Observe-se que, dado um inteiro n , apenas nos interessa considerar, para a prova, o caso em que n é ímpar, ou seja, assumimos que p é verdadeira e procuramos mostrar que também q é verdadeira.

demonstração: Pretendemos mostrar que, se $n \in \mathbb{Z}$ é um número ímpar, então existem $a, b \in \mathbb{Z}$ tais que $n = a^2 - b^2$.

Suponhamos, então, que $n \in \mathbb{Z}$ é um número ímpar.

Então, existe um $k \in \mathbb{Z}$ tal que $n = 2k + 1$.

Ora,

$$n = 2k + 1 = k^2 + 2k + 1 - k^2 = (k + 1)^2 - k^2 = a^2 - b^2,$$

com $a = k + 1$ e $b = k$ inteiros. Logo, n escreve-se como a diferença de dois quadrados perfeitos. ■

1.4.4 Prova de uma equivalência

Atendendo à equivalência lógica $(p \leftrightarrow q) \Leftrightarrow ((p \rightarrow q) \wedge (q \rightarrow p))$, a prova de uma afirmação do tipo $p \leftrightarrow q$ pode passar pela prova de duas implicações.

Na prova de $p \leftrightarrow q$, constrói-se uma prova de $p \rightarrow q$ e uma prova de $q \rightarrow p$.

[Exemplo]

Consideremos a seguinte afirmação sobre $n \in \mathbb{Z}$: n^2 é par se e só se n é par.

Esta proposição pode ser escrita na forma $p \leftrightarrow q$, onde

p : n^2 é par.

e

q : n é par.

Observe-se que, dizer que n^2 é par é equivalente a afirmar que $n^2 = 2k$ para algum inteiro k . Logo, $n = \pm\sqrt{2k}$, o que não nos permite concluir nada sobre a paridade de n . A prova da equivalência dada passa pela prova de $p \rightarrow q$ e de $q \rightarrow p$. Esta última é trivial:

demonstração [$q \rightarrow p$]: Admitamos a veracidade de q e procuremos provar p . Para tal, admitamos que n é par. Por definição, existe, então, um inteiro k tal que $n = 2k$. Logo, $n^2 = (2k)^2$, donde $n^2 = 2(2k^2)$, ou seja, $n^2 = 2s$, com $s = 2k^2 \in \mathbb{Z}$. Concluimos, deste modo, que n^2 é par, isto é, p é verdadeira. ■

A prova de $p \leftrightarrow q$ só fica completa quando formos capazes de provar a implicação $p \rightarrow q$. Veremos essa prova na secção 1.4.8.

1.4.5 Prova de uma negação

Na prova de $\neg p$, assume-se p e procura-se uma contradição.

[Exemplo]

Consideremos a proposição: Não existem $n, m \in \mathbb{N}$ tais que $2n + 16m = 13$. Facilmente se verifica que esta é a negação da proposição

$$p: \text{Existem } n, m \in \mathbb{N} \text{ tais que } 2n + 16m = 13.$$

Para provar a veracidade de $\neg p$, mostramos que p não pode, de facto, ser verdadeira:

demonstração: Suponhamos que existem números naturais n e m tais que $2n + 16m = 13$. Então,

$$13 = 2n + 16m = 2(n + 8m),$$

pelo que 13 é divisível por 2, o que contradiz o facto de 13 ser um número ímpar.

Assim, não existem $n, m \in \mathbb{N}$ tais que $2n + 16m = 13$. ■

1.4.6 Prova indireta por contradição ou redução ao absurdo

Para provar uma afirmação p , assume-se $\neg p$ e procura-se uma contradição.

No exemplo que se segue, apresenta-se uma demonstração do resultado enunciado recorrendo a uma prova por redução ao absurdo.

[Exemplo]

Proposição: Existe uma infinidade de números primos.

demonstração: No sentido de provarmos por contradição este resultado, admitamos que existe um número finito de primos, digamos p_1, p_2, \dots, p_n , com $n \in \mathbb{N}$.

Considere-se, agora, o número

$$x = p_1 p_2 \cdots p_n + 1.$$

Temos que

$$x = p_1 \times (p_2 \cdots p_n) + 1,$$

pelo que o resto da divisão de x por p_1 é 1 e, por conseguinte, x não é divisível por p_1 .

Analogamente,

$$x = p_2 \times (p_1 p_3 \cdots p_n) + 1,$$

donde o resto da divisão de x por p_2 é, também, 1 e, por isso, x não é divisível por p_2 .

É óbvio que este raciocínio se pode aplicar com qualquer um dos primos p_1, \dots, p_n e, portanto, podemos concluir que o número x não é divisível por nenhum dos números primos p_1, p_2, \dots, p_n (pois o resto da divisão é sempre 1).

Logo, x é um número primo, o que contradiz a hipótese inicial de que existem apenas n números primos, uma vez que x é diferente de qualquer um dos números de entre p_1, \dots, p_n .

Então a hipótese inicial está errada e, portanto, existe um número infinito de primos.

■

1.4.7 Prova de uma implicação por redução ao absurdo

Muitas proposições matemáticas são enunciadas na forma de uma implicação $p \rightarrow q$. Para além destas, existem outras proposições que, embora não sendo implicações, a sua prova pode passar pela demonstração de uma afirmação do tipo $p \rightarrow q$.

Por estes motivos, é conveniente conhecer e estudar diversos métodos de prova indireta que existem para uma implicação.

A prova de $p \rightarrow q$ pode ser feita por contradição. Uma vez que $p \rightarrow q$ é logicamente equivalente a $\neg(p \wedge \neg q)$, temos que $\neg(p \rightarrow q)$ é logicamente equivalente a $p \wedge \neg q$.

[Exemplo]

Consideremos o seguinte resultado que garante a unicidade da inversa de uma matriz invertível sobre o corpo dos complexos.

[Teorema] Seja A uma matriz quadrada de ordem n , sobre \mathbb{C} , invertível. Então, existe uma única matriz X , também de ordem n , sobre \mathbb{C} , tal que $AX = XA = I_n$, onde I_n é a matriz identidade de ordem n .

O enunciado deste teorema é da forma $p \rightarrow q$, onde

p : A é uma matriz quadrada de ordem n , sobre \mathbb{C} , invertível.

e

q : Existe uma única matriz X , de ordem n , sobre \mathbb{C} , tal que $AX = XA = I_n$, onde I_n é a matriz identidade de ordem n .

A prova de $p \rightarrow q$ por redução ao absurdo passa por assumir-se $p \wedge \neg q$ e procurar-se uma contradição. Ora, ao assumirmos $p \wedge \neg q$, estamos a assumir p e $\neg q$. Sendo p verdadeira, fica garantida a existência de pelo menos uma matriz X , de ordem n , sobre \mathbb{C} , tal que $AX = XA = I_n$, onde I_n é a matriz identidade de ordem n . Sendo assim, afirmar que $\neg q$ é verdadeira é equivalente a dizer que existe mais do que uma matriz nessas condições e isso leva a uma contradição:

demonstração: Sendo A uma matriz invertível, sabemos que existe uma matriz X de ordem n , sobre \mathbb{C} , tal que $AX = XA = I_n$. Admitamos que X não é única, ou seja, que existe uma outra matriz quadrada Y , de ordem n , sobre \mathbb{C} , tal que $AY = YA = I_n$. Então,

$$Y = YI_n = Y(AX) = (YA)X = I_nX = X,$$

o que é absurdo. Logo, existe uma só matriz X nas condições referidas. ■.

[Exemplo]

Consideremos a seguinte proposição: Se $x \in \mathbb{R}$ é tal que $x^2 = 2$, então $x \notin \mathbb{Q}$.

Esta proposição é da forma $p \rightarrow q$, onde

$$p: x \in \mathbb{R} \text{ e } x^2 = 2$$

e

$$q: x \notin \mathbb{Q}$$

e é equivalente a afirmar que $\sqrt{2}$ e $-\sqrt{2}$ são números irracionais.

A seguinte prova da proposição segue por redução absurdo:

demonstração: Suponhamos que $x \in \mathbb{R}$ é tal que $x^2 = 2$ e $x \in \mathbb{Q}$, e procuremos uma contradição.

Ora, se $x^2 = 2$ temos que $x = \sqrt{2}$ ou $x = -\sqrt{2}$. Consideremos o caso em que $x = \sqrt{2}$ (o outro caso é análogo).

Então, $\sqrt{2} = x \in \mathbb{Q}$, pelo que existem $a, b \in \mathbb{Z}$ tais que $b \neq 0$, m.d.c.(a, b) = 1 e

$$x = \frac{a}{b}.$$

Assim,

$$2 = x^2 = \left(\frac{a}{b}\right)^2 = \frac{a^2}{b^2},$$

pelo que $a^2 = 2b^2$.

Logo, a^2 é um número par e, consequentemente, a também o é. Portanto, existe $k \in \mathbb{N}$ tal que $a = 2k$.

Assim, $(2k)^2 = 2b^2$ ou, equivalentemente,

$$4k^2 = 2b^2,$$

pelo que $b^2 = 2k^2$.

Então, b^2 é par e b também o é.

Como a e b são pares, 2 é divisor de ambos os números, contrariando o facto de $\text{m.d.c.}(a, b) = 1$. ■

1.4.8 Prova de uma implicação por contraposição ou por contrarrecíproco

Atendendo a que as fórmulas $p \rightarrow q$ e $\neg q \rightarrow \neg p$ são logicamente equivalentes, a demonstração de um resultado do primeiro tipo pode ser feita, indiretamente, apresentando uma prova de $\neg q \rightarrow \neg p$. A uma tal demonstração chama-se prova por contraposição ou por contrarrecíproco.

Para demonstrar uma afirmação do tipo $p \rightarrow q$, assume-se $\neg q$ e encontra-se uma prova de $\neg p$.

[Exemplo]

Consideremos o exemplo apresentado na secção 1.4.4, onde se procurava apresentar uma prova da seguinte afirmação sobre $n \in \mathbb{Z}$: n^2 é par se e só se n é par.

Como referimos, esta proposição pode ser escrita na forma $p \leftrightarrow q$, onde

$$p: n^2 \text{ é par.}$$

e

$$q: n \text{ é par.}$$

A fim de completar a prova desta proposição apresentada nesse exemplo, resta provar a implicação $p \rightarrow q$. Note-se que não é possível uma prova direta de tal implicação:

demonstração: Iremos demonstrar este resultado por contraposição. Nesse sentido, suponhamos que n não é par, ou seja, que n é ímpar.

Então, existe $k \in \mathbb{N}$ tal que $n = 2k + 1$, pelo que $n^2 = (2k + 1)^2 = 4k^2 + 4k + 1 = 2(2k^2 + 2k) + 1$. Logo, n^2 é ímpar. ■

Observe-se que a prova acima é a demonstração da implicação $\neg q \rightarrow \neg p$. Sendo esta proposição equivalente a $p \rightarrow q$, a prova acima é também uma demonstração de $p \rightarrow q$.

1.4.9 Prova indireta de uma disjunção

Como já referimos anteriormente, a prova de uma disjunção pode também ser feita de um modo indireto.

Uma vez que ambas as fórmulas $\neg p \rightarrow q$ e $\neg q \rightarrow p$ são logicamente equivalentes a $p \vee q$, a prova da disjunção de p e q pode passar pela prova de $\neg p \rightarrow q$ ou de $\neg q \rightarrow p$.

Na prova de $p \vee q$, assume-se $\neg p$ e procura-se uma prova de q ou, equivalentemente, assume-se $\neg q$ e procura-se uma prova de p .

[Exemplo]

Consideremos a seguinte proposição: Dados dois números reais x e y tais que $xy = 0$, temos $x = 0$ ou $y = 0$.

Considerando \mathbb{R} o universo de variação das variáveis, esta proposição pode ser escrita na forma $r \rightarrow (p \vee q)$, onde

$$r: xy = 0,$$

$$p: x = 0$$

e

$$q: y = 0.$$

Para provar a proposição dada, assumimos r e procuramos uma prova de $p \vee q$. Será na prova de $p \vee q$ que usaremos o método de prova descrito nesta secção.

demonstração: Pretendemos mostrar que $x = 0$ ou $y = 0$, assumindo que $x, y \in \mathbb{R}$ e $xy = 0$. Iremos demonstrar esta disjunção recorrendo a uma prova indireta. Nesse sentido, começamos por supor que $x \neq 0$ e procuramos concluir que $y = 0$.

Sendo x um número real não nulo, $\frac{1}{x} \in \mathbb{R}$. Logo,

$$xy = 0 \Leftrightarrow \frac{1}{x}(xy) = \frac{1}{x}.0 \Leftrightarrow \left(\frac{1}{x}x\right)y = 0 \Leftrightarrow 1.y = 0 \Leftrightarrow y = 0. \blacksquare$$

1.4.10 Prova por casos

A prova direta de uma afirmação do tipo $(p_1 \vee \dots \vee p_n) \rightarrow q$ consiste em procurar uma prova de q assumindo $p_1 \vee \dots \vee p_n$. Para que $p_1 \vee \dots \vee p_n$ seja verdadeira, é necessário que pelo menos uma das proposições p_i seja verdadeira. Assim, podemos construir a prova estudando cada um dos casos possíveis: (1) p_1 é verdadeira; (2) p_2 é verdadeira; ...; (n) p_n é verdadeira. A uma tal prova dá-se o nome de **prova por casos**.

A prova por casos de uma afirmação do tipo $(p_1 \vee \dots \vee p_n) \rightarrow q$ consiste em procurar uma prova para cada uma das implicações $p_1 \rightarrow q$, ..., $p_n \rightarrow q$.

[Exemplo]

Consideremos a seguinte proposição: Se a e b são números reais tais que $0 \leq a < b$, então $a^2 < b^2$.

A prova que apresentamos considera dois casos possíveis para a : $a > 0$ e $a = 0$.

demonstração: Sejam $a, b \in \mathbb{R}$ tais que $0 \leq a < b$. Pretendemos mostrar que $a^2 < b^2$. Uma vez que $0 \leq a$, a prova será feita considerando dois casos: $a > 0$ e $a = 0$.

[i] Se $a > 0$, então $a < b$ implica que $a \times a < a \times b$ ou, equivalentemente, $a^2 < ab$. Como $b > 0$, também $a < b$ implica que $a \times b < b \times b$ ou, equivalentemente, $ab < b^2$. Logo, $a^2 < ab < b^2$.

[ii] Se $a = 0$, então $a^2 = 0^2 = 0$ e $ab = 0 \times b = 0$. Como $b > 0$, de $a < b$ concluímos que $a \times b < b \times b$ ou, equivalentemente, $ab < b^2$. Assim, $a^2 = 0 = ab < b^2$. ■

1.4.11 Prova de uma proposição com quantificador universal

Na prova direta de uma proposição do tipo “ $\forall x p(x)$ ”, admitimos que a variável a representa um elemento arbitrário do universo de quantificação U da variável x e mostramos que $p(a)$ é verdadeira.

No caso em que U é um conjunto finito, podemos optar por uma **prova por exaustão**, testando individualmente, para cada $a \in U$, se $p(a)$ é verdadeira.

[Exemplo]

Consideremos a seguinte quantificação universal: Dado um número natural n , $n^2 + n$ é par.

Sendo o universo de variação de n um conjunto infinito, a argumentação da verdade da proposição dada não pode passar pela atribuição de valores concretos a n . A ideia é mostrar que $n^2 + n$ é um número par para qualquer valor que n possa tomar.

demonstração: Pretendemos mostrar que $\forall_{n \in \mathbb{N}} n^2 + n$ é par. Admitamos que a representa um valor arbitrário em \mathbb{N} e procuremos mostrar que $a^2 + a$ é par.

Se a for par, então a^2 é par. Como a soma de dois números pares é ainda um número par, $a^2 + a$ é par.

Por outro lado, se a for ímpar, então a^2 é ímpar. Ora, a soma de dois números ímpares é um número par, pelo que $a^2 + a$ é par. ■

[Exemplo]

Consideremos a seguinte quantificação universal sobre um universo finito: Todo o elemento de $U = \{4, 16, 49\}$ é um quadrado perfeito.

Pretendemos mostrar que $\forall_{n \in U} n$ é um quadrado perfeito. Sendo o universo de variação de n um conjunto finito, a argumentação da veracidade da proposição passa por uma prova por exaustão:

demonstração: Recorde-se que um quadrado perfeito é um inteiro da forma k^2 com $k \in \mathbb{Z}$. Dado que os elementos de U são 4, 16 e 49 e dado que $4 = 2^2$, $16 = 4^2$ e $49 = 7^2$, podemos concluir que todo o elemento de U é um quadrado perfeito. ■

1.4.12 Prova de uma proposição com quantificador existencial

Na prova direta de uma proposição do tipo “ $\exists_x p(x)$ ”, é necessário exibir um elemento a do universo de quantificação U da variável x tal que $p(a)$ seja verdadeira.

Este tipo de prova diz-se uma **prova construtiva**.

[Exemplo]

Consideremos a seguinte proposição: A equação $x^5 - x^4 - 2\sqrt{2}x^3 + 2\sqrt{2}x^2 + 2x - 2 = 0$ admite uma solução inteira.

Pretendemos mostrar que $\exists_{x \in \mathbb{Z}} x^5 - x^4 - 2\sqrt{2}x^3 + 2\sqrt{2}x^2 + 2x - 2 = 0$. Numa prova direta, basta apresentar um valor inteiro a tal que $a^5 - a^4 - 2\sqrt{2}a^3 + 2\sqrt{2}a^2 + 2a - 2 = 0$:

demonstração: Consideremos $a = 1 \in \mathbb{Z}$. Então, $a^5 - a^4 - 2\sqrt{2}a^3 + 2\sqrt{2}a^2 + 2a - 2 = 1 - 1 - 2\sqrt{2} + 2\sqrt{2} + 2 - 2 = 0$, pelo que 1 é solução da equação em causa. ■

Em certos casos, a prova construtiva não é simples ou não é possível, podendo-se optar por uma prova indireta por contradição. Nesta situação, a prova diz-se **não construtiva**.

1.4.13 Prova de existência e unicidade

A prova direta de uma proposição do tipo “ $\exists_x^1 p(x)$ ” pode ser dividida em duas partes:

[prova de existência] prova-se que existe, pelo menos, um elemento a do universo de quantificação de x tal que $p(a)$ é verdade;

[prova de unicidade] supõe-se que a e b são dois elementos do universo de quantificação de x tais que $p(a)$ e $p(b)$ são verdadeiras e mostra-se que $a = b$.

[Exemplo]

Consideremos a seguinte proposição: Existe um elemento neutro para a multiplicação em \mathbb{R} e esse elemento é único.

Pretendemos mostrar que $\exists_{u \in \mathbb{R}}^1 \forall_{x \in \mathbb{R}} xu = ux = x$.

Na prova que apresentamos de seguida, começamos por mostrar que existe pelo menos um elemento u que satisfaz $\forall_{x \in \mathbb{R}} xu = ux = x$. De seguida, mostramos que esse elemento é único.

[prova de existência] Consideremos $u = 1 \in \mathbb{R}$. Pretendemos mostrar que $\forall_{x \in \mathbb{R}} xu = ux = x$. Ora, dado $x \in \mathbb{R}$, $xu = x \times 1 = x = 1 \times x = ux$.

Logo, $u = 1$ é elemento neutro para a multiplicação.

[prova de unicidade] Suponhamos agora que $u' \in \mathbb{R}$ é elemento neutro para a multiplicação. Então, $1 = 1 \times u'$. Por outro lado, 1 é elemento neutro para a multiplicação e, portanto, $u' = 1 \times u'$. Logo, $u' = 1$. ■

1.4.14 Prova de falsidade de uma quantificação universal por contraexemplo

A prova de falsidade de uma proposição do tipo “ $\forall_x p(x)$ ” passa por mostrar que existe um elemento a do universo de quantificação tal que $p(a)$ é falsa.

Neste caso, diz-se que a é um **contraexemplo** para a proposição “ $\forall_x p(x)$ ”.

[Exemplo]

Consideremos a seguinte quantificação universal: Todo o número real admite inverso para a multiplicação.

É afirmado que $\forall_{x \in \mathbb{R}} \exists_{y \in \mathbb{R}} xy = 1$. Consideremos $a = 0 \in \mathbb{R}$ e mostremos que a proposição “ $\exists_{y \in \mathbb{R}} ay = 1$ ” é falsa.

Temos, pois, de mostrar que “ $\forall_{y \in \mathbb{R}} ay \neq 1$ ” é verdadeira.

Ora, dado $y \in \mathbb{R}$, $ay = 0 \times y = 0 \neq 1$.

Assim, 0 é um contraexemplo para a proposição considerada. ■

1.5 Exercícios resolvidos

1. Considere as fórmulas $\varphi : p_1 \leftrightarrow (\neg p_1 \vee p_2)$ e $\psi : (p_1 \rightarrow (\neg p_1 \vee p_2)) \wedge ((p_1 \wedge \neg p_2) \rightarrow \neg p_1)$. Diga, justificando, se cada uma das afirmações que se seguem é ou não verdadeira.
 - (a) Se o valor lógico da fórmula φ é 1, então os valores lógicos das variáveis proposicionais p_1 e p_2 são iguais.
 - (b) As fórmulas φ e ψ são logicamente equivalentes.

resolução:

(a) Sabemos que o valor lógico de φ é 1 se e somente se os valores lógicos de p_1 e de $(\neg p_1 \vee p_2)$ são iguais. Ora, se p_1 é verdadeira, então, para $(\neg p_1 \vee p_2)$ ser verdadeira, p_2 tem de ser verdadeira. Por outro lado, se p_1 é falsa, então $(\neg p_1 \vee p_2)$ é verdadeira, independentemente do valor lógico de p_2 . Logo, se p_1 é falsa, o valor lógico de φ é 0. Assim, se o valor lógico de φ é 1, então p_1 e p_2 são ambas verdadeiras e a afirmação é verdadeira.

[observação: esta alínea podia ser resolvida com a análise da tabela de verdade de φ]

(b) Consideremos a tabela de verdade

p_1	p_2	$\neg p_1$	$\neg p_2$	$\neg p_1 \vee p_2$	φ	$p_1 \rightarrow (\neg p_1 \vee p_2)$	$p_1 \wedge \neg p_2$	$(p_1 \wedge \neg p_2) \rightarrow \neg p_1$	ψ
1	1	0	0	1	1	1	0	1	1
1	0	0	1	0	0	0	1	0	0
0	1	1	0	1	0	1	0	1	1
0	0	1	1	1	0	1	0	1	1

Os valores lógicos de φ e de ψ nem sempre são iguais. Logo, as fórmulas não são logicamente equivalentes e a afirmação é falsa.

2. Verifique se a fórmula $\varphi : (p_0 \vee \neg p_1) \leftrightarrow (\neg p_0 \rightarrow p_1)$ é uma tautologia.

resolução: Consideremos a tabela de verdade de φ :

p_0	p_1	$\neg p_0$	$\neg p_1$	$p_0 \vee \neg p_1$	$\neg p_0 \rightarrow p_1$	φ
1	1	0	0	1	1	1
1	0	0	1	1	1	1
0	1	1	0	0	1	0
0	0	1	1	1	0	0

Como o valor lógico de φ não é sempre 1, podemos concluir que φ não é uma tautologia.

3. Considerando que A é um subconjunto de \mathbb{Z} , que p representa a proposição $\forall_{y \in A} \exists_{x \in A} y = x^2$ e que q representa a proposição $\exists_{y \in A} \forall_{x \in A} y = x^2$,

- (a) Dê exemplo de A para o qual apenas uma das proposições p, q é verdadeira. Justifique.
- (b) Indique, sem recorrer ao conetivo *negação*, uma proposição equivalente a $\neg p$.

resolução:

(a) Para p ser verdadeira, para todo $y \in A$ tem de existir $x \in A$ tal que $y = x^2$, ou seja, para todo $y \in A$, $\sqrt{y} \in A$ ou $-\sqrt{y} \in A$. Note-se que os elementos de A são números inteiros.

Para q ser verdadeira, tem de existir $y \in A$ que seja igual aos quadrados de todos os valores de $x \in A$.

Começemos por apresentar um conjunto A em que p é falsa e q é verdadeira. Consideremos $A = \{-1, 1\}$. Para $y = -1$ não existe $x \in A$ tal que $y = x^2$. Logo, p é falsa. Note-se que $y = 1$ é tal que $y = (-1)^2$ e $y = 1^2$. Assim, q é verdadeira.

Vejamos, agora, um exemplo de um conjunto A em que p é verdadeira e q é falsa. Seja $A = \{0, 1\}$. Para $y = 0$ existe $x \in A$ tal que $y = x^2$: basta considerar $x = 0$. Para $y = 1$ existe $x \in A$ tal que $y = x^2$: basta considerar $x = 1$. Portanto, p é verdadeira. Como não existe nenhum $y \in A$ que seja igual aos quadrados de todos os elementos de A , q é falsa. Note-se que $0^2 = 0 \neq 1 = 1^2$.

(b) Recorde-se que $\neg \forall y \in A \exists x \in A r(x, y) \Leftrightarrow \exists y \in A \forall x \in A \neg r(x, y)$.

Sendo assim,

$$\exists y \in A \forall x \in A y \neq x^2$$

é logicamente equivalente a $\neg p$.

4. Considerando que p representa a proposição

$$\exists y \in A \forall x \in A (x \neq y \rightarrow (xy > 0 \vee x^2 + y = 0)),$$

(a) Justificando, dê exemplo de um universo A não vazio onde:

- (i) a proposição p é verdadeira;
- (ii) a proposição p é falsa.

(b) Indique, sem recorrer ao conetivo *negação*, uma proposição equivalente a $\neg p$.

resolução:

(a)(i) Para p ser verdadeira, tem de existir um elemento y em A tal que, para todos os valores de x em A distintos de y , $xy > 0$ ou $x^2 + y = 0$. Tomemos, por exemplo, $A = \{-2, -1, 1\}$ e consideremos $y = -1$.

Para $x = -2$, a proposição $(xy > 0 \vee x^2 + y = 0)$ é verdadeira, uma vez que $xy = 2 > 0$. Para $x = 1$, a proposição $(xy > 0 \vee x^2 + y = 0)$ é, também, verdadeira, uma vez que $xy = -1 < 0$ mas $x^2 + y = 1^2 - 1 = 0$. Assim, para $A = \{-2, -1, 1\}$, p é verdadeira.

(ii) Para p ser falsa, para todo o valor de y em A tem de existir pelo menos um valor de x em A , distinto de y , tal que a proposição $(xy > 0 \vee x^2 + y = 0)$ é falsa, ou seja, tal que $xy \leq 0$ e $x^2 + y \neq 0$.

Tomemos, por exemplo, $A = \{-1, 0\}$. Consideremos $y = -1$.

Para $x = 0$, a proposição $(xy > 0 \vee x^2 + y = 0)$ é falsa, uma vez que $xy = 0 \not> 0$ e $x^2 + y = -1 \neq 0$. Consideremos, agora, $y = 0$. Para $x = -1$, a proposição $(xy > 0 \vee x^2 + y = 0)$ é, também, falsa, pois $xy = 0 \not> 0$ e $x^2 + y = 1 \neq 0$. Logo, p é falsa para $A = \{-1, 0\}$.

(b) Recorde-se que $\neg \exists y \in A \forall x \in A r(x, y) \Leftrightarrow \forall y \in A \exists x \in A \neg r(x, y)$, que $\neg(\varphi \rightarrow \psi) \Leftrightarrow (\varphi \wedge \neg\psi)$ e que $\neg(\varphi \vee \psi) \Leftrightarrow (\neg\varphi \wedge \neg\psi)$.

Sendo assim,

$$\forall y \in A \exists x \in A (x \neq y \wedge (xy \leq 0 \wedge x^2 + y \neq 0))$$

é logicamente equivalente a $\neg p$.

5. Sejam p e q proposições. Diga, justificando, se a seguinte afirmação é ou não verdadeira: Para provar que $p \rightarrow q$ é verdadeira, é necessário provar que q é verdadeira.

resolução: A afirmação é falsa. De facto, $p \rightarrow q$ pode ser verdadeira e q ser falsa: de facto, se p e q forem ambas falsas, a implicação $p \rightarrow q$ é verdadeira.

Consideremos, por exemplo, a proposição “Se hoje é sábado, amanhã é domingo”. Esta proposição é verdadeira. No entanto, a proposição “Amanhã é domingo” não tem de ser verdadeira.

6. Sejam p e q proposições. Diga, justificando, se a seguinte afirmação é ou não verdadeira: Para mostrar que $p \wedge q$ é falsa, basta mostrar que se p é verdadeira, então q é falsa.

resolução: A afirmação é verdadeira. Efetivamente, para $p \wedge q$ ser falsa, pelo menos uma das proposições p ou q tem de ser falsa. Se p for falsa, automaticamente $p \wedge q$ é falsa, independentemente do valor lógico de q . Sendo assim, o único caso que tem de ser analisado é o caso em que p é verdadeira. Nesse caso, para $p \wedge q$ ser falsa, q tem de ser falsa. Assim, para mostrar que $p \wedge q$ é falsa, basta mostrar que se p é verdadeira, então q é falsa.

7. Prove que se n é um número natural ímpar, então $2n^2 + 4n - 14$ é múltiplo de 8.

resolução: Admitamos que n é um número natural ímpar. Então, existe $k \in \mathbb{N}_0$ tal que $n = 2k + 1$. Logo,

$$\begin{aligned}
2n^2 + 4n - 14 &= 2 \times (2k + 1)^2 + 4 \times (2k + 1) - 14 \\
&= 2 \times (4k^2 + 4k + 1) + (8k + 4) - 14 \\
&= 8k^2 + 8k + 2 + 8k + 4 - 14 \\
&= 8k^2 + 16k - 8 \\
&= 8 \times (k^2 + 2k - 1)
\end{aligned}$$

Note-se que $k^2 + 2k - 1 \in \mathbb{Z}$. Logo, $2n^2 + 4n - 14$ é múltiplo de 8, pois é da forma $8r$ para algum $r \in \mathbb{Z}$.

8. Prove que se o produto de dois números naturais m e n é ímpar, então m e n têm a mesma paridade.

resolução: A prova segue por contrarrecíproca. Provaremos, então, que se m e n têm paridades distintas, o produto mn é par. Para tal, admitamos que m e n são números naturais que não têm a mesma paridade. Então um destes números é par e o outro ímpar. Suponhamos que m é par e que n é ímpar (o outro caso é análogo). Nesse caso, existe $k \in \mathbb{N}$ tal que $m = 2k$ e existe $r \in \mathbb{N}_0$ tal que $n = 2r + 1$. Assim,

$$\begin{aligned}
mn &= (2k) \times (2r + 1) \\
&= 4kr + 2k \\
&= 2 \times (2kr + k)
\end{aligned}$$

Como $2kr + k \in \mathbb{N}$, segue-se que mn é par.

9. Seja n um número natural. Mostre que se $n^2 + 8n - 1$ é divisível por 4, então n é ímpar.

resolução: A prova segue por contrarrecíproca. Provaremos, então, que se n é par, então $n^2 + 8n - 1$ não é divisível por 4. Admitamos que n é par. Então, existe $k \in \mathbb{N}$ tal que $n = 2k$. Logo,

$$\begin{aligned}
n^2 + 8n - 1 &= (2k)^2 + 8 \times (2k) - 1 \\
&= 4k^2 + 16k - 1 \\
&= 4k^2 + 16k - 4 + 3 \\
&= 4 \times (k^2 + 4k - 1) + 3
\end{aligned}$$

Como $k^2 + 4k - 1 \in \mathbb{N}$, segue-se que o resto da divisão inteira de $n^2 + 8n - 1$ por 4 é 3 e, portanto, $n^2 + 8n - 1$ não é divisível por 4.

Capítulo 2

Teoria elementar de conjuntos

A noção de conjunto é uma noção fundamental na Matemática. O estudo de conjuntos (designado por **Teoria de Conjuntos**) foi introduzido por Georg Cantor, nos finais do século XIX. A teoria de Cantor, um tanto intuitiva, foi posteriormente tratada de uma forma axiomática.

A Teoria de Conjuntos revela-se, hoje, essencial não só em muitos campos da matemática, mas também noutras áreas como as ciências da computação.

2.1 Noções básicas

Nesta unidade curricular, iremos considerar a noção de conjunto como um conceito primitivo, ou seja, como uma noção intuitiva, a partir da qual serão definidas outras noções.

[Definição 2.1] Intuitivamente, um **conjunto** é uma coleção de objetos, designados **elementos** ou **membros** do conjunto.

[Exemplo]

São exemplos de conjuntos as coleções de:

- i | unidades curriculares do primeiro ano do plano de estudos do MiEInf;
- ii | pessoas presentes numa festa;
- iii | estações do ano;
- iv | todos os números naturais.

Representamos os conjuntos por letras maiúsculas A, B, C, \dots, X, Y, Z , eventualmente com índices. Os elementos de um conjunto são habitualmente representados por letras minúsculas a, b, c, \dots, x, y, z , também eventualmente com índices.

[Definição 2.2] Sejam A um conjunto e x um objeto. Dizemos que x **pertence a** A , e escrevemos $x \in A$, se x é um dos objetos de A . Caso x não seja um dos objetos de A , dizemos que x **não pertence a** A e escrevemos $x \notin A$.

[Exemplo]

Sejam A o conjunto de todos os números primos inferiores a 50 e B o conjunto de todas as soluções da equação $x^2 + 3x - 4 = 0$. Temos, por exemplo, que $3 \in A$ e $1 \in B$. Por outro lado, $1 \notin A$ e $3 \notin B$.

Um conjunto pode ser descrito de diversas formas. Podemos descrever um conjunto enumerando explicitamente os seus elementos, colocando-os entre chavetas e separados por vírgulas. Neste caso, dizemos que o conjunto é descrito **por extensão**.

[Exemplo]

Se A é o conjunto de todos os números primos inferiores a 50 e B o conjunto de todas as soluções da equação $x^2 + 3x - 4 = 0$, então A e B podem ser descritos por extensão do seguinte modo: $A = \{2, 3, 5, 7, 11, 13, 17, 19, 23, 29, 31, 37, 41, 43, 47\}$ e $B = \{-4, 1\}$

Numa descrição por extensão, nem sempre é possível ou praticável a enumeração de todos os elementos. Nesse caso, utiliza-se uma notação sugestiva e não ambígua que permita intuir os elementos não expressos.

[Exemplo]

O conjunto dos números naturais é usualmente representado por extensão utilizando a seguinte notação: $\mathbb{N} = \{1, 2, 3, \dots\}$.

O conjunto dos números inteiros pode ser escrito por extensão recorrendo à seguinte notação: $\mathbb{Z} = \{\dots, -3, -2, -1, 0, 1, 2, 3, \dots\}$.

Podemos descrever um conjunto indicando um predicado $p(x)$, com domínio de variação U para a variável x , tal que os valores possíveis a em U para os quais $p(a)$ é verdadeira são exatamente os elementos do conjunto em causa. Neste caso, a condição $p(x)$ caracteriza totalmente os elementos do conjunto e dizemos que o conjunto é descrito **por compreensão**.

[Exemplo]

O conjunto dos números naturais menores do que 5 pode ser descrito, por extensão, por $\{1, 2, 3, 4\}$. Em alternativa, podemos definir esse conjunto por compreensão como se segue: $\{n \in \mathbb{N} : n < 5\}$.

[Exemplo]

Seja $X = \{-2, -\sqrt{2}, -1, 0, 1, \sqrt{2}, 2, 4\}$. Consideremos os seguintes conjuntos definidos por compreensão: $A = \{x \in X : x \in \mathbb{N}\}$, $B = \{x \in X : |x| < 2\}$, $C = \{x \in X : \sqrt{x} \in X\}$, $D = \{x^2 : x \in X\}$ e $E = \{x \in X : x^2 \in X\}$.

Note-se que o conjunto A é o conjunto formado pelos elementos x de X tais que $x \in \mathbb{N}$. Ora, os únicos elementos de X que são números naturais são o 1, o 2 e o 4. Assim, $A = \{1, 2, 4\}$.

O conjunto B é formado pelos elementos x de X tais que $|x| < 2$. Como

$$\begin{array}{ll} |-2| = 2 \not< 2 & |-\sqrt{2}| = \sqrt{2} < 2 \\ |-1| = 1 < 2 & |0| = 0 < 2 \\ |1| = 1 < 2 & |\sqrt{2}| = \sqrt{2} < 2 \\ |2| = 2 \not< 2 & |4| = 4 \not< 2 \end{array}$$

temos que os elementos de X cujo valor absoluto é inferior a 2 são: $-\sqrt{2}$, -1 , 0 , 1 e $\sqrt{2}$. Logo, $B = \{-\sqrt{2}, -1, 0, 1, \sqrt{2}\}$.

Por definição, C é o conjunto formado pelos elementos de X cuja raiz quadrada é, também, um elemento de X . Ora,

$$\begin{array}{ll} \sqrt{-2} \notin X & \sqrt{-\sqrt{2}} \notin X \\ \sqrt{-1} \notin X & \sqrt{0} = 0 \in X \\ \sqrt{1} = 1 \in X & \sqrt{\sqrt{2}} \notin X \\ \sqrt{2} \in X & \sqrt{4} = 2 \in X \end{array}$$

Podemos, então, afirmar que os elementos de X cuja raiz quadrada é, também, um elemento de X são os seguintes: 0 , 1 , 2 e 4 . Portanto, $C = \{0, 1, 2, 4\}$.

O conjunto D é formado pelos valores de x^2 onde $x \in X$. Por outras palavras, D é o conjunto dos quadrados dos elementos de X . Sendo

$$\begin{array}{ll} (-2)^2 = 4 & (-\sqrt{2})^2 = 2 \\ (-1)^2 = 1 & 0^2 = 0 \\ 1^2 = 1 & (\sqrt{2})^2 = 2 \\ 2^2 = 4 & 4^2 = 16 \end{array}$$

segue-se que $D = \{0, 1, 2, 4, 16\}$.

O conjunto E é o conjunto dos elementos x de X tais que x^2 é, também, um elemento de X . Dado que

$$\begin{array}{ll} (-2)^2 = 4 \in X & (-\sqrt{2})^2 = 2 \in X \\ (-1)^2 = 1 \in X & 0^2 = 0 \in X \\ 1^2 = 1 \in X & (\sqrt{2})^2 = 2 \in X \\ 2^2 = 4 \in X & 4^2 = 16 \notin X \end{array}$$

temos que $E = \{-2, -\sqrt{2}, -1, 0, 1, \sqrt{2}, 2\}$.

[Definição 2.3] Ao único conjunto que não tem qualquer elemento chamamos **conjunto vazio**, e representamo-lo por \emptyset ou por $\{\}$.

O conjunto vazio pode ser descrito por compreensão, recorrendo a um predicado que não possa ser satisfeito. Por exemplo, $\emptyset = \{n \in \mathbb{N} : n^2 = 28\} = \{x : x \neq x\}$.

[Definição 2.4] Dois conjuntos A e B dizem-se **iguais**, e escreve-se $A = B$, se têm os mesmos elementos, ou seja, se $\forall x (x \in A \leftrightarrow x \in B)$. Se existir um elemento num dos conjuntos que não pertence ao outro, então A e B dizem-se **diferentes**.

[Exemplo]

O conjunto de todos os divisores naturais de 4 é igual ao conjunto $A = \{1, 2, 4\}$ e também é igual ao conjunto $B = \{x \in \mathbb{R} : x^3 - 7x^2 + 14x - 8 = 0\}$.

Os conjuntos $C = \{x \in \mathbb{N} : x \text{ é múltiplo de } 3\}$ e $D = \{6, 12, 18, 24, \dots\}$ são diferentes, pois $3 \in C$ e $3 \notin D$.

Quando se pretende provar a igualdade entre dois conjuntos X e Y dos quais não conhecemos uma definição por extensão, o processo passa por mostrar que, para todo o x , $x \in X$ se e só se $x \in Y$ [ex.: ver exercício resolvido 8. deste capítulo].

[Definição 2.5] Sejam A e B conjuntos. Diz-se que A **está contido em** B ou que A é **um subconjunto de** B , e escreve-se $A \subseteq B$, se todo o elemento de A é também elemento de B , ou seja, se $\forall x (x \in A \rightarrow x \in B)$. Se existir um elemento de A que não é elemento de B , ou seja, se $\exists_{x \in A} x \notin B$, diz-se que A **não está contido em** B ou que A **não é um subconjunto de** B , e escreve-se $A \not\subseteq B$.

[Exemplo]

$\{-1, 1\} \subseteq \{x \in \mathbb{R} : x^3 - 2x^2 - x + 2 = 0\}$, uma vez que tanto -1 como 1 são soluções da equação $x^3 - 2x^2 - x + 2 = 0$.

$\{0, -1, 1\} \not\subseteq \{x \in \mathbb{R} : x^3 - 2x^2 - x + 2 = 0\}$, uma vez que 0 não é solução da equação $x^3 - 2x^2 - x + 2 = 0$, pelo que 0 pertence ao primeiro conjunto mas não ao segundo.

Quando se pretende provar a inclusão de um conjunto X num conjunto Y dos quais não conhecemos uma definição por extensão, o processo passa por mostrar que, para todo o x , se $x \in X$ então $x \in Y$ [ex.: ver exercício resolvido 7. deste capítulo].

[Definição 2.6] Sejam A e B conjuntos. Diz-se que A **está propriamente contido em** B ou que A é **um subconjunto próprio de** B , e escreve-se $A \subsetneq B$ ou $A \subset B$, se $A \subseteq B$ e $A \neq B$, ou seja, se

$$\forall x (x \in A \rightarrow x \in B) \quad \wedge \quad \exists_{x \in B} x \notin A.$$

[Exemplo]

$\{-1, 1\} \subsetneq \{x \in \mathbb{R} : x^3 - 2x^2 - x + 2 = 0\}$, uma vez que, para além de 1 e -1, 2 também é solução da equação $x^3 - 2x^2 - x + 2 = 0$.

[Proposição 2.7] Sejam A , B e C conjuntos. Então,

- 1 | $\emptyset \subseteq A$;
- 2 | $A \subseteq A$;
- 3 | Se $A \subseteq B$ e $B \subseteq C$ então $A \subseteq C$;
- 4 | $A = B$ se e só se $(A \subseteq B \text{ e } B \subseteq A)$.

demonstração:

1 | Mostremos, por redução ao absurdo, que $\emptyset \subseteq A$. Nesse sentido, assumamos que $\emptyset \not\subseteq A$. Então, existe um elemento de \emptyset que não pertence a A . Ora, \emptyset não tem elementos. Esta contradição resultou de supormos que $\emptyset \not\subseteq A$. Logo, $\emptyset \subseteq A$.

2 | Dado um elemento arbitrário a de A , é claro que $a \in A$. Logo, $\forall_x (x \in A \rightarrow x \in A)$, ou seja, $A \subseteq A$.

3 | Suponhamos que $A \subseteq B$ e $B \subseteq C$, ou seja,

$$(*) \forall_x (x \in A \rightarrow x \in B) \quad \text{e} \quad (**) \forall_x (x \in B \rightarrow x \in C).$$

Pretendemos mostrar que $A \subseteq C$, isto é, $\forall_x (x \in A \rightarrow x \in C)$. Seja $x \in A$. Por (*), podemos concluir que $x \in B$. Logo, de (**), vem que $x \in C$. Assim, todo o elemento de A é elemento de C , ou seja, $A \subseteq C$.

4 | Pretendemos mostrar a veracidade da equivalência $A = B$ se e só se $(A \subseteq B \text{ e } B \subseteq A)$. Iremos fazê-lo provando as duas implicações.

(\Rightarrow) Suponhamos que $A = B$. Então,

$$\forall_x (x \in A \leftrightarrow x \in B),$$

ou, equivalentemente,

$$\forall_x ((x \in A \rightarrow x \in B) \wedge (x \in B \rightarrow x \in A)).$$

Logo, $A \subseteq B$ e $B \subseteq A$.

(\Leftarrow) Suponhamos que $A \subseteq B$ e $B \subseteq A$. Então, todo o elemento de A é elemento de B e todo o elemento de B é elemento de A . Por outras palavras, A e B têm exatamente os mesmos elementos, ou seja, $A = B$. ■

2.2 Operações com conjuntos: união, interseção e complementação

[Definição 2.8] Sejam A e B subconjuntos de um conjunto X (dito o **universo**). Chama-se **união** ou **reunião de A com B** , e representa-se por $A \cup B$, o conjunto cujos elementos são os elementos de A e os elementos de B , ou seja,

$$A \cup B = \{x \in X : x \in A \vee x \in B\}.$$

Dado $x \in X$, temos que $x \in A \cup B$ se e só se $x \in A \vee x \in B$ e temos que $x \notin A \cup B$ se e só se $x \notin A \wedge x \notin B$.

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$. Então, $A \cup B = \{1, 2, 3, 4, 5\}$.

[2] Sejam $C = \{2n : n \in \mathbb{N}\}$ e $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Então, $C \cup D = \{n \in \mathbb{N} : n \text{ é par } \vee n \leq 10\}$.

[Definição 2.9] Sejam A e B subconjuntos de um conjunto X . Chama-se **interseção de A com B** , e representa-se por $A \cap B$, o conjunto cujos elementos pertencem a ambos os conjuntos A e B , ou seja,

$$A \cap B = \{x \in X : x \in A \wedge x \in B\}.$$

Dado $x \in X$, temos que $x \in A \cap B$ se e só se $x \in A \wedge x \in B$ e temos que $x \notin A \cap B$ se e só se $x \notin A \vee x \notin B$.

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$. Então, $A \cap B = \{3\}$.

[2] Sejam $C = \{2n : n \in \mathbb{N}\}$ e $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Então, $C \cap D = \{2, 4, 6, 8, 10\}$.

[Definição 2.10] Sejam A e B subconjuntos de um conjunto X . Chama-se **complementar de B em A** , e representa-se por $A \setminus B$, o conjunto cujos elementos pertencem a A mas não pertencem a B , ou seja,

$$A \setminus B = \{x \in X : x \in A \wedge x \notin B\}.$$

O complementar de B em A também se designa por **diferença de A com B** e representa-se por $A - B$.

Dado $x \in X$, temos que $x \in A \setminus B$ se e só se $x \in A \wedge x \notin B$ e temos que $x \notin A \setminus B$ se e só se $x \notin A \vee x \in B$.

Quando A é o universo X , o conjunto $A \setminus B = X \setminus B$ diz-se o **complementar de B** e representa-se por \overline{B} ou B' .

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$ e $B = \{3, 4, 5\}$. Então, $A \setminus B = \{1, 2\}$.

[2] Sejam $C = \{2n : n \in \mathbb{N}\}$ e $D = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10\}$. Então, $C \setminus D = \{n \in \mathbb{N} : n \text{ é par} \wedge n > 10\}$ e $\mathbb{N} \setminus D = \{n \in \mathbb{N} : n > 10\}$.

[3] Dados os subconjuntos $E = \{-2, 0, 2, \pi, 7\}$ e $F =]-\infty, 3]$ de \mathbb{R} , temos $E \cup F =]-\infty, 3] \cup \{\pi, 7\}$, $E \cap F = \{-2, 0, 2\}$, $E \setminus F = \{\pi, 7\}$ e $\overline{E \cup F} = [3, \pi[\cup]\pi, 7[\cup]7, +\infty[$.

Na proposição que se segue, apresentam-se algumas propriedades relativas à união de conjuntos.

[Proposição 2.11] Sejam A , B e C subconjuntos de um conjunto X . Então,

- 1 | $A \subseteq A \cup B$ e $B \subseteq A \cup B$;
- 2 | $A \cup \emptyset = A$;
- 3 | $A \cup A = A$;
- 4 | $A \cup X = X$;
- 5 | $A \cup B = B \cup A$;
- 6 | $(A \cup B) \cup C = A \cup (B \cup C)$;
- 7 | se $A \subseteq B$ então $A \cup B = B$.

demonstração: Iremos demonstrar as propriedades 1, 2, 4, 6 e 7. As restantes ficam como exercício.

1 | Mostremos que $A \subseteq A \cup B$, ou seja, que

$$\forall_x (x \in A \rightarrow x \in A \cup B).$$

Seja $x \in A$. Então, é verdadeira a proposição $x \in A \vee x \in B$, pelo que $x \in A \cup B$. Logo, se $x \in A$ então $x \in A \cup B$ e, portanto, $A \subseteq A \cup B$.

A prova de $B \subseteq A \cup B$ é análoga.

2 | Mostremos que $A \cup \emptyset = A$. Da propriedade 1, vem que $A \subseteq A \cup \emptyset$. Resta, pois, provar que $A \cup \emptyset \subseteq A$.

Seja $x \in A \cup \emptyset$. Então, $x \in A \vee x \in \emptyset$.

Ora, a proposição $x \in \emptyset$ é falsa, pois \emptyset não tem elementos. Logo, podemos concluir que $x \in A$ e, portanto, se $x \in A \cup \emptyset$, então $x \in A$. Por outras palavras, $A \cup \emptyset \subseteq A$.

Assim, $A \cup \emptyset = A$.

4 | Provemos agora que $A \cup X = X$. Da propriedade 1, vem que $X \subseteq A \cup X$. Basta mostrar que $A \cup X \subseteq X$.

Seja $x \in A \cup X$. Então, $x \in A \vee x \in X$. Pretendemos mostrar que $x \in X$. Podemos dividir a prova em dois casos: (I) $x \in A$; (II) $x \in X$.

No caso (I), como A é um subconjunto de X , temos que todo o elemento de A é também elemento de X . Portanto, $x \in X$. No caso (II), é imediato que $x \in X$.

Logo, se $x \in A \cup X$, então $x \in X$, donde $A \cup X \subseteq X$ e, assim, $A \cup X = X$.

6 | Mostremos que $(A \cup B) \cup C = A \cup (B \cup C)$. Por definição de união de conjuntos,

$$x \in (A \cup B) \cup C \Leftrightarrow x \in A \cup B \vee x \in C \Leftrightarrow (x \in A \vee x \in B) \vee x \in C.$$

Uma vez que é válida a propriedade associativa para a disjunção (ver proposição 1.10), temos que

$$(x \in A \vee x \in B) \vee x \in C \Leftrightarrow x \in A \vee (x \in B \vee x \in C).$$

Novamente pela definição de união de conjuntos, temos

$$x \in A \vee (x \in B \vee x \in C) \Leftrightarrow x \in A \vee x \in B \cup C \Leftrightarrow x \in A \cup (B \cup C).$$

Logo, $x \in (A \cup B) \cup C \Leftrightarrow x \in A \cup (B \cup C)$, pelo que $(A \cup B) \cup C = A \cup (B \cup C)$.

7 | Admitamos que $A \subseteq B$ e mostremos que $A \cup B = B$. Da propriedade 1, vem que $B \subseteq A \cup B$. Falta, pois, provar que $A \cup B \subseteq B$.

Seja $x \in A \cup B$. Então, $x \in A \vee x \in B$. Podemos dividir a prova em dois casos: (I) $x \in A$; (II) $x \in B$.

No caso (I), como A é um subconjunto de B , sabemos que todo o elemento de A é também elemento de B . Portanto, $x \in B$. No caso (II), é imediato que $x \in B$.

Assim, se $x \in A \cup B$, então $x \in B$.

Logo, $A \cup B \subseteq B$, pelo que $A \cup B = B$. ■

Em seguida, apresentamos algumas propriedades relativas à interseção de conjuntos.

[Proposição 2.12] Sejam A , B e C subconjuntos de um conjunto X . Então,

- 1 | $A \cap B \subseteq A$ e $A \cap B \subseteq B$;
- 2 | $A \cap \emptyset = \emptyset$;
- 3 | $A \cap A = A$;
- 4 | $A \cap X = A$;
- 5 | $A \cap B = B \cap A$;
- 6 | $(A \cap B) \cap C = A \cap (B \cap C)$;
- 7 | se $A \subseteq B$ então $A \cap B = A$.

demonstração Iremos demonstrar as propriedades 1, 2 e 7. As restantes ficam como exercício.

1 | Mostremos que $A \cap B \subseteq A$, ou seja, que $\forall_x (x \in A \cap B \rightarrow x \in A)$. Seja $x \in A \cap B$. Então, por definição de interseção de conjuntos, $x \in A \wedge x \in B$. Logo, são verdadeiras ambas as

proposições $x \in A$ e $x \in B$. Em particular, $x \in A$ é uma proposição verdadeira. Assim, se $x \in A \cap B$, então $x \in A$ e, portanto, $A \cap B \subseteq A$.

A prova de $A \cap B \subseteq B$ é análoga.

2 | Mostremos que $A \cap \emptyset = \emptyset$. Façamo-lo por redução ao absurdo, admitindo que $A \cap \emptyset \neq \emptyset$.

Então, existe um objeto x tal que $x \in A \cap \emptyset$.

Logo, $x \in A \wedge x \in \emptyset$. Em particular, $x \in \emptyset$. Mas \emptyset não tem elementos, pelo que temos um absurdo, que resultou de supormos que $A \cap \emptyset \neq \emptyset$.

Assim, $A \cap \emptyset = \emptyset$.

7 | Admitamos que $A \subseteq B$ e mostremos que $A \cap B = A$. Da propriedade 1, vem que $A \cap B \subseteq A$. Falta, pois, provar que $A \subseteq A \cap B$.

Seja $x \in A$. Então, como $A \subseteq B$, podemos concluir que $x \in B$.

Logo, temos $x \in A \wedge x \in B$. Vimos, portanto, que se $x \in A$, então $x \in A \wedge x \in B$, ou seja, se $x \in A$, então $x \in A \cap B$.

Assim, $A \subseteq A \cap B$. ■

Vejamos algumas propriedades relacionadas com a complementação.

[Proposição 2.13] Sejam A , B e C subconjuntos de um conjunto X . Então,

- 1 | $A \cap \overline{A} = \emptyset$ e $A \cup \overline{A} = X$;
- 2 | $A \setminus \emptyset = A$ e $A \setminus X = \emptyset$;
- 3 | se $A \subseteq B$, então $A \setminus B = \emptyset$;
- 4 | $A \setminus (B \cup C) = (A \setminus B) \cap (A \setminus C)$;
- 5 | $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$;
- 6 | $\overline{A \cup B} = \overline{A} \cap \overline{B}$;
- 7 | $\overline{A \cap B} = \overline{A} \cup \overline{B}$;
- 8 | $\overline{(\overline{A})} = A$.

demonstração: Iremos provar as propriedades 1, 2 e 5. As restantes ficam como exercício.

1 | Começemos por mostrar que $A \cap \overline{A} = \emptyset$ por redução ao absurdo. Suponhamos, pois, que existe $x \in A \cap \overline{A}$. Então,

$$x \in A \wedge x \in \overline{A}.$$

Logo, por definição de complementar de um conjunto,

$$x \in A \wedge (x \in X \wedge x \notin A).$$

Chegamos, desta forma, a uma contradição, $x \in A \wedge x \notin A$, que resultou de supormos que $A \cap \overline{A} \neq \emptyset$. Portanto, $A \cap \overline{A} = \emptyset$.

Verifiquemos, agora, que $A \cup \overline{A} = X$.

Dado $x \in A \cup \overline{A}$, temos $x \in A \vee x \in \overline{A}$. Temos, deste modo, dois casos a considerar: (I) $x \in A$; (II) $x \in \overline{A}$. Como A e \overline{A} são subconjuntos de X , os elementos de cada um desses conjuntos são, ainda, elementos de X . Assim, em ambos os casos podemos afirmar que $x \in X$.

Portanto, $A \cup \overline{A} \subseteq X$.

Resta mostrar que $X \subseteq A \cup \overline{A}$. Nesse sentido, tomemos $x \in X$.

É claro que a proposição $x \in A \vee x \notin A$ é verdadeira. Ora, se $x \in X$ e $x \notin A$, então $x \in \overline{A}$.

Logo,

$$\text{se } x \in X, \text{ então } x \in A \vee x \in \overline{A},$$

ou seja,

$$\text{se } x \in X, \text{ então } x \in A \cup \overline{A}.$$

Portanto, $X \subseteq A \cup \overline{A}$ e a igualdade pretendida segue.

2 | Começemos por mostrar que $A \setminus \emptyset = A$.

Por definição, $A \setminus \emptyset$ é o conjunto de todos os elementos de A que não pertencem a \emptyset . Ora, nenhum elemento pertence a \emptyset .

Logo, $A \setminus \emptyset$ é o conjunto de todos os elementos de A , ou seja, $A \setminus \emptyset = A$.

No sentido de provar, por redução ao absurdo, que $A \setminus X = \emptyset$, tomemos $x \in A \setminus X$.

Então, x é tal que $x \in A \wedge x \notin X$.

Como A é um subconjunto de X ,

$$\text{se } x \in A, \text{ então } x \in X.$$

Portanto, x é tal que $x \in X \wedge x \notin X$, uma contradição. Assim, $A \setminus X = \emptyset$.

5 | Pretendemos mostrar que $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. Precisamos, pois, de mostrar que $x \in A \setminus (B \cap C)$ se e somente se $x \in (A \setminus B) \cup (A \setminus C)$, para todo o objeto x .

Ora, pelas leis de De Morgan e pela propriedade distributiva da operação lógica \wedge em relação à operação \vee , temos que, para qualquer objeto x ,

$$\begin{aligned} x \in A \setminus (B \cap C) &\Leftrightarrow x \in A \wedge x \notin (B \cap C) \\ &\Leftrightarrow x \in A \wedge \neg(x \in B \cap C) \\ &\Leftrightarrow x \in A \wedge \neg(x \in B \wedge x \in C) \\ &\Leftrightarrow x \in A \wedge (\neg(x \in B) \vee \neg(x \in C)) \\ &\Leftrightarrow x \in A \wedge (x \notin B \vee x \notin C) \\ &\Leftrightarrow (x \in A \wedge x \notin B) \vee (x \in A \wedge x \notin C) \\ &\Leftrightarrow (x \in A \setminus B) \vee (x \in A \setminus C) \\ &\Leftrightarrow x \in (A \setminus B) \cup (A \setminus C) \end{aligned}$$

Logo, $A \setminus (B \cap C) = (A \setminus B) \cup (A \setminus C)$. ■

[Observação] Sejam A_1, A_2, \dots, A_n subconjuntos de um conjunto X . Tendo em conta que as operações de união e de interseção de conjuntos gozam da propriedade associativa, podemos escrever sem ambiguidade

$$A_1 \cup A_2 \cup \dots \cup A_n$$

e

$$A_1 \cap A_2 \cap \dots \cap A_n.$$

A união dos conjuntos A_1, A_2, \dots, A_n é usualmente notada por $\bigcup_{i=1}^n A_i$ e a interseção por $\bigcap_{i=1}^n A_i$. Assim,

$$\bigcup_{i=1}^n A_i = \{x \in X : x \in A_1 \vee x \in A_2 \vee \dots \vee x \in A_n\}$$

e

$$\bigcap_{i=1}^n A_i = \{x \in X : x \in A_1 \wedge x \in A_2 \wedge \dots \wedge x \in A_n\}.$$

2.3 Conjunto das partes de um conjunto

[Definição 2.14] Seja A um conjunto. Chamamos **conjunto das partes de A** ou **conjunto potência de A** , que representamos por $\mathcal{P}(A)$, ao conjunto de todos os subconjuntos de A , ou seja,

$$\mathcal{P}(A) = \{X : X \subseteq A\}.$$

[Exemplo]

Consideremos o conjunto $A = \{1, 2, 3\}$. Usando, no máximo, estes três elementos, que conjuntos podemos formar? O conjunto sem nenhum elemento (\emptyset), os conjuntos com apenas um dos três elementos (especificamente, $\{1\}$, $\{2\}$ e $\{3\}$), os conjuntos com exatamente dois desses três elementos (concretamente, $\{1, 2\}$, $\{1, 3\}$ e $\{2, 3\}$) e o conjunto formado pelos três elementos ($\{1, 2, 3\}$). Note-se que estes são os elementos de $\mathcal{P}(A)$. Com efeito, $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$.

[Exemplo]

Sejam $A = \{a, b, c\}$, $B = \{1, 2\}$, $C = \{1, \{2\}\}$ e $D = \emptyset$. Então,

$$1 \mid \mathcal{P}(A) = \{\emptyset, \{a\}, \{b\}, \{c\}, \{a, b\}, \{a, c\}, \{b, c\}, \{a, b, c\}\}$$

$$2 \mid \mathcal{P}(B) = \{\emptyset, \{1\}, \{2\}, \{1, 2\}\}$$

$$3 \mid \mathcal{P}(C) = \{\emptyset, \{1\}, \{\{2\}\}, \{1, \{2\}\}\}$$

$$4 \mid \mathcal{P}(\emptyset) = \{\emptyset\}$$

[Proposição 2.15] Sejam A e B dois conjuntos. Então,

- 1 | $\emptyset \in \mathcal{P}(A)$ e $A \in \mathcal{P}(A)$;
- 2 | se $A \subseteq B$, então $\mathcal{P}(A) \subseteq \mathcal{P}(B)$;
- 3 | se A tem n elementos, então $\mathcal{P}(A)$ tem 2^n elementos.

demonstração:

1 | Para qualquer conjunto A , temos que $\emptyset \subseteq A$ e $A \subseteq A$, pelo que \emptyset e A são elementos de $\mathcal{P}(A)$.

2 | Suponhamos que $A \subseteq B$. Pretendemos mostrar que $\mathcal{P}(A) \subseteq \mathcal{P}(B)$, ou seja,

$$\forall X (X \in \mathcal{P}(A) \rightarrow X \in \mathcal{P}(B)).$$

Seja $X \in \mathcal{P}(A)$. Então, $X \subseteq A$. Pela proposição 2.7, como $X \subseteq A$ e $A \subseteq B$, podemos concluir que $X \subseteq B$.

Logo, $X \in \mathcal{P}(B)$ e, portanto, $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

3 | consultar bibliografia adequada.

2.4 Produto cartesiano de conjuntos

Dados dois objetos a e b , os conjuntos $\{a, b\}$ e $\{b, a\}$ são iguais, uma vez que têm exatamente os mesmos elementos. A ordem pela qual são listados os elementos não interessa.

Em certas situações, interessa considerar os objetos por determinada ordem. Para tal, recorreremos ao conceito de par ordenado.

[Definição 2.16] Dados dois objetos a e b , o **par ordenado de a e de b** será denotado por (a, b) . Dois pares ordenados (a, b) e (c, d) dizem-se **iguais**, escrevendo-se $(a, b) = (c, d)$, quando $a = c$ e $b = d$.

Note-se que, dados dois objetos a e b , se $a \neq b$, então $(a, b) \neq (b, a)$.

Num par ordenado (a, b) , o objeto a é designado por **primeira coordenada** (ou **primeira componente**) e o objeto b é designado por **segunda coordenada** (ou **segunda componente**).

Os pares ordenados permitem-nos formar novos conjuntos a partir de conjuntos dados.

[Definição 2.17] Sejam A e B conjuntos. O conjunto de todos os pares ordenados (a, b) tais que $a \in A$ e $b \in B$ diz-se o **produto cartesiano de A por B** e representa-se por $A \times B$. Ou seja,

$$A \times B = \{(a, b) : a \in A \wedge b \in B\}.$$

Dado um objeto x , temos que $x \in A \times B$ se e só se existem $a \in A$ e $b \in B$ tais que $x = (a, b)$.
 Dado um par (u, v) , temos que $(u, v) \in A \times B$ se e só se $u \in A \wedge v \in B$ e temos que $(u, v) \notin A \times B$ se e só se $u \notin A \vee v \notin B$.

[Exemplos]

- [1] Sejam $A = \{1, 2\}$ e $B = \{a, b, c\}$. Então,
 $A \times B = \{(1, a), (1, b), (1, c), (2, a), (2, b), (2, c)\}$
 $B \times A = \{(a, 1), (a, 2), (b, 1), (b, 2), (c, 1), (c, 2)\}$.

É claro que $A \times B \neq B \times A$.

- [2] Sejam $C = \{2n : n \in \mathbb{N}\}$ e $D = \{2n + 1 : n \in \mathbb{N}\}$. Então,
 $C \times D = \{(2n, 2m + 1) : n, m \in \mathbb{N}\}$.

- [3] Sejam $E = F = \mathbb{R}$. Os elementos de $E \times F = \mathbb{R} \times \mathbb{R}$ podem ser representados geometricamente como pontos de um plano munido de um eixo de coordenadas.

A noção de produto cartesiano de dois conjuntos generaliza-se de forma natural:

[Definição 2.18] Sejam A_1, A_2, \dots, A_n conjuntos ($n \geq 2$). O *produto cartesiano* de A_1, A_2, \dots, A_n , notado por $A_1 \times A_2 \times \dots \times A_n$, é o conjunto dos n -úplos ordenados (a_1, a_2, \dots, a_n) em que $a_1 \in A_1, a_2 \in A_2, \dots, a_n \in A_n$, ou seja,

$$A_1 \times A_2 \times \dots \times A_n = \{(a_1, a_2, \dots, a_n) : a_1 \in A_1 \wedge a_2 \in A_2 \wedge \dots \wedge a_n \in A_n\}.$$

Se $A_1 = A_2 = \dots = A_n = A$, escrevemos A^n em alternativa a $A \times A \times \dots \times A$.

[Observação] Dois n -úplos ordenados (a_1, a_2, \dots, a_n) e (b_1, b_2, \dots, b_n) são iguais se e somente se $a_1 = b_1$ e $a_2 = b_2$ e \dots e $a_n = b_n$.

[Exemplo]

Sejam $A = \{4, 5\}$, $B = \{1, 2, 3\}$ e $C = \{7\}$. Temos que

$$A \times B \times C = \{(4, 1, 7), (4, 2, 7), (4, 3, 7), (5, 1, 7), (5, 2, 7), (5, 3, 7)\}$$

e

$$A^2 = \{(4, 4), (4, 5), (5, 4), (5, 5)\}.$$

Vejamos algumas propriedades relacionadas com o produto cartesiano.

Proposição 2.19 Sejam A, B, C e D conjuntos. Então,

- 1 | $A \times \emptyset = \emptyset = \emptyset \times A$;
- 2 | sendo os conjuntos não vazios, $(A \times B) \subseteq (C \times D)$ se e só se $A \subseteq C$ e $B \subseteq D$;
- 3a | $C \times (A \cup B) = (C \times A) \cup (C \times B)$;

$$3b \mid (A \cup B) \times C = (A \times C) \cup (B \times C);$$

$$4a \mid C \times (A \cap B) = (C \times A) \cap (C \times B);$$

$$4b \mid (A \cap B) \times C = (A \times C) \cap (B \times C);$$

$$5a \mid C \times (A \setminus B) = (C \times A) \setminus (C \times B);$$

$$5b \mid (A \setminus B) \times C = (A \times C) \setminus (B \times C).$$

demonstração:

2 | Admitamos que todos os conjuntos são não vazios. Pretendemos mostrar que $(A \times B) \subseteq (C \times D)$ se e só se $A \subseteq C$ e $B \subseteq D$.

(\Rightarrow) Suponhamos que $(A \times B) \subseteq (C \times D)$ e procuremos provar que $A \subseteq C$ e $B \subseteq D$.

Sejam $a \in A$ e $b \in B$. Então, por definição de produto cartesiano, $(a, b) \in A \times B$.

Por hipótese, todo o elemento de $A \times B$ é elemento de $C \times D$.

Portanto, $(a, b) \in C \times D$, pelo que $a \in C$ e $b \in D$.

Provámos, assim, que

$$\forall_a (a \in A \rightarrow a \in C) \quad \text{e} \quad \forall_b (b \in B \rightarrow b \in D),$$

ou seja, $A \subseteq C$ e $B \subseteq D$.

(\Leftarrow) Reciprocamente, admitamos que $A \subseteq C$ e $B \subseteq D$ e mostremos que $(A \times B) \subseteq (C \times D)$.

Seja $(a, b) \in A \times B$. Então, por definição de produto cartesiano, $a \in A$ e $b \in B$.

Por hipótese, todo o elemento de A é elemento de C e todo o elemento de B é elemento de D .

Logo, $a \in C$ e $b \in D$ e, portanto, $(a, b) \in C \times D$. Assim,

$$\forall_{a,b} ((a, b) \in A \times B \rightarrow (a, b) \in C \times D)$$

e, portanto, $(A \times B) \subseteq (C \times D)$.

5a | Pretendemos mostrar que $C \times (A \setminus B) = (C \times A) \setminus (C \times B)$.

Dado um par ordenado (x, y) ,

$$\begin{aligned} (x, y) \in (C \times A) \setminus (C \times B) &\Leftrightarrow (x, y) \in C \times A \wedge (x, y) \notin C \times B \\ &\Leftrightarrow (x \in C \wedge y \in A) \wedge (x \notin C \vee y \notin B) \\ &\Leftrightarrow ((x \in C \wedge y \in A) \wedge x \notin C) \vee \\ &\quad \vee ((x \in C \wedge y \in A) \wedge y \notin B) \\ &\Leftrightarrow (x \in C \wedge y \in A) \wedge y \notin B \\ &\Leftrightarrow x \in C \wedge (y \in A \wedge y \notin B) \\ &\Leftrightarrow x \in C \wedge y \in (A \setminus B) \\ &\Leftrightarrow (x, y) \in C \times (A \setminus B) \end{aligned}$$

A demonstração das restantes propriedades fica como exercício. ■

[Observação] Se os conjuntos A_1, A_2, \dots, A_n têm p_1, p_2, \dots, p_n elementos, respetivamente, o produto cartesiano $A_1 \times A_2 \times \dots \times A_n$ tem $p_1 \times p_2 \times \dots \times p_n$ elementos.

2.5 Exercícios resolvidos

1. Considere os conjuntos $A = \{3, \{4\}\}$, $B = \{3, 4, 15\}$, $C = \{n \in \mathbb{Z} \mid n^2 - 1 \in B\}$ e $D = \{(x, y) \in \mathbb{Z} \times \mathbb{Z} \mid x \in A \wedge x = 3|y|\}$.

(a) Determine C e D .

(b) Verifique se $(A \times B) \setminus \{(3, 4), (4, 3)\} \subseteq \mathbb{N} \times \mathbb{N}$.

(c) Determine $\mathcal{P}(A) \cap \mathcal{P}(B)$.

resolução:

- (a) Temos que $n^2 - 1 \in B$ se e só se $n^2 - 1 = 3$ ou $n^2 - 1 = 4$ ou $n^2 - 1 = 15$. Ora,

$$\begin{aligned} n^2 - 1 = 3 &\Leftrightarrow n^2 = 4 \\ &\Leftrightarrow n = \pm 2 \end{aligned}$$

$$\begin{aligned} n^2 - 1 = 4 &\Leftrightarrow n^2 = 5 \\ &\Leftrightarrow n = \pm\sqrt{5} \end{aligned}$$

$$\begin{aligned} n^2 - 1 = 15 &\Leftrightarrow n^2 = 16 \\ &\Leftrightarrow n = \pm 4 \end{aligned}$$

Como $\pm 2 \in \mathbb{Z}$, $\pm\sqrt{5} \notin \mathbb{Z}$ e $\pm 4 \in \mathbb{Z}$, $C = \{-4, -2, 2, 4\}$.

Quanto ao conjunto D , note-se que é formado pelos pares ordenados (x, y) em que $x, y \in \mathbb{Z}$ são tais que $x \in A$ e $x = 3|y|$. Ora, para $x \in \mathbb{Z}$ ser tal que $x \in A$, x tem de ser igual a 3. Assim,

$$\begin{aligned} x = 3|y| &\Leftrightarrow 3 = 3|y| \\ &\Leftrightarrow |y| = 1 \\ &\Leftrightarrow y = \pm 1 \end{aligned}$$

Como $1 \in \mathbb{Z}$ e $-1 \in \mathbb{Z}$, temos que $D = \{(3, -1), (3, 1)\}$.

(b) Note-se que a inclusão será válida se e somente se todos os elementos de $(A \times B) \setminus \{(3, 4), (4, 3)\}$ forem elementos de $\mathbb{N} \times \mathbb{N}$, ou, equivalentemente, se as coordenadas de todos os pares de $(A \times B) \setminus \{(3, 4), (4, 3)\}$ forem números naturais. Ora, $(\{4\}, 3) \in (A \times B)$ e, como $(\{4\}, 3) \notin \{(3, 4), (4, 3)\}$, $(\{4\}, 3) \in (A \times B) \setminus \{(3, 4), (4, 3)\}$. Como a primeira coordenada do par ordenado $(\{4\}, 3)$ não é um número natural, podemos concluir que $(A \times B) \setminus \{(3, 4), (4, 3)\} \not\subseteq \mathbb{N} \times \mathbb{N}$.

(c) Por definição, $X \in \mathcal{P}(A) \cap \mathcal{P}(B)$ se e só se $X \in \mathcal{P}(A)$ e $X \in \mathcal{P}(B)$, isto é, se e só se $X \subseteq A$ e $X \subseteq B$. Ora, os únicos subconjuntos comuns a A e a B são \emptyset e $\{3\}$. Assim, $\mathcal{P}(A) \cap \mathcal{P}(B) = \{\emptyset, \{3\}\}$.

2. Considere os conjuntos $A = \{\{1, 3\}, 1, 4\}$, $B = \{-3, 1, 3\}$ e $C = \{x \in \mathbb{Z} : 2|x| + 1 \in B\}$.

- (a) **Determine** $A \setminus B$.
- (b) **Determine** $\mathcal{P}(A \cap C)$.
- (c) **Verifique se** $\{-1, 3\} \subseteq C \cup B$.
- (d) $\{1, 3\} \in A \cap \mathcal{P}(A)$? **Justifique.**

resolução:

(a) Temos que $A \setminus B = \{x \mid x \in A \wedge x \notin B\}$. Ora, o único elemento de A que também é elemento de B é o 1. Assim, $A \setminus B = \{\{1, 3\}, 4\}$.

(b) Começemos por determinar C . Temos que $2|x| + 1 \in B$ se e somente se $2|x| + 1 = -3$ ou $2|x| + 1 = 1$ ou $2|x| + 1 = 3$. Atendendo a que

$$\begin{aligned} 2|x| + 1 = -3 &\Leftrightarrow 2|x| = -4 \\ &\Leftrightarrow |x| = -2 \\ &\Leftrightarrow i(x) \end{aligned}$$

$$\begin{aligned} 2|x| + 1 = 1 &\Leftrightarrow 2|x| = 0 \\ &\Leftrightarrow |x| = 0 \\ &\Leftrightarrow x = 0 \end{aligned}$$

$$\begin{aligned} 2|x| + 1 = 3 &\Leftrightarrow 2|x| = 2 \\ &\Leftrightarrow |x| = 1 \\ &\Leftrightarrow x = \pm 1, \end{aligned}$$

podemos concluir que $C = \{-1, 0, 1\}$. Assim, $A \cap C = \{1\}$ e $\mathcal{P}(A \cap C) = \{\emptyset, \{1\}\}$.

(c) Por definição de inclusão, $\{-1, 3\} \subseteq C \cup B$ se e somente se -1 e 3 são elementos de $C \cup B$. Como $C \cup B = \{x \mid x \in C \vee x \in B\}$ e $-1 \in C$ e $3 \in B$, podemos concluir que $\{-1, 3\} \subseteq C \cup B$.

(d) $\{1, 3\} \in A \cap \mathcal{P}(A)$ se e só se $\{1, 3\} \in A$ e $\{1, 3\} \in \mathcal{P}(A)$. Sabemos que $\{1, 3\}$ é um dos elementos de A , pelo que, efetivamente, $\{1, 3\} \in A$. Para $\{1, 3\}$ ser um dos elementos de $\mathcal{P}(A)$, teríamos de ter $\{1, 3\} \subseteq A$, o que não é verdade pois $3 \in \{1, 3\}$ mas $3 \notin A$. Logo, $\{1, 3\} \notin A \cap \mathcal{P}(A)$.

3. Considere os conjuntos $A = \{2n \mid n \in \mathbb{N} \wedge n^3 \leq 40\}$, $B = \{1, \{2, 4\}\}$, $C = \{1, 2, 4\}$ e $D = \{x \in \mathbb{Z} \mid x^2 - 3 \in B\}$.

(a) **Determine** A e D .

(b) **Verifique se** $(1, \{2, 4\}, 4) \in C \times (B \setminus C) \times C$. **Justifique.**

(c) **Verifique se** $B \cap \mathcal{P}(C) = \emptyset$. **Justifique.**

resolução:

(a) Temos que, dado $n \in \mathbb{N}$, $n^3 \leq 40$ se e só se $n \in \{1, 2, 3\}$. Assim, $A = \{2 \times 1, 2 \times 2, 2 \times 3\} = \{2, 4, 6\}$.

Definamos, agora, por extensão, o conjunto D .

Temos que, dado $x \in \mathbb{Z}$, $x^2 - 3 \in B$ se e somente se $x^2 - 3 = 1$. Ora,

$$\begin{aligned} x^2 - 3 = 1 &\Leftrightarrow x^2 = 4 \\ &\Leftrightarrow x = \pm 2. \end{aligned}$$

Assim, $D = \{-2, 2\}$.

(b) $(1, \{2, 4\}, 4) \in C \times (B \setminus C) \times C$ se e só se $1 \in C$, $\{2, 4\} \in B \setminus C$ e $4 \in C$.

Como $1 \in C$, $\{2, 4\} \in B$, $\{2, 4\} \notin C$ e $4 \in C$, segue-se que $(1, \{2, 4\}, 4) \in C \times (B \setminus C) \times C$.

(c) Temos que $B \cap \mathcal{P}(C) = \emptyset$ se nenhum elemento de B pertencer a $\mathcal{P}(C)$.

É óbvio que $1 \notin \mathcal{P}(C)$, mas $\{2, 4\} \in B$ e $\{2, 4\} \subseteq C$. Logo, $\{2, 4\} \in B \cap \mathcal{P}(C)$ e, portanto, $B \cap \mathcal{P}(C) \neq \emptyset$.

4. Dê exemplo de ou justifique que não existem conjuntos A , B e/ou C tais que

(a) $(1, 2, 1) \in A \times B \times C$.

(b) $A \cup B = A \cap B$.

(c) $B \subseteq C$ e $A \cap \overline{C} \not\subseteq A \cap \overline{B}$.

resolução:

(a) Por definição de produto cartesiano, $(1, 2, 1) \in A \times B \times C$ se e só se $1 \in A$, $2 \in B$ e $1 \in C$. Consideremos, por exemplo, $A = \{1\}$, $B = \{2\}$ e $C = \{1\}$.

(b) Sabemos que $A \cup A = A \cap A = A$, para qualquer conjunto A . Assim, para $A = B = \{1\}$, por exemplo, temos $A \cup B = A \cap B$.

(c) Admitamos que A, B e C são tais que $B \subseteq C$ e $A \cap \overline{C} \not\subseteq A \cap \overline{B}$. Como $A \cap \overline{C} \not\subseteq A \cap \overline{B}$, existe pelo menos um objeto x tal que $x \in A \cap \overline{C}$ e $x \notin A \cap \overline{B}$. Ora,

$$\begin{aligned} x \in A \cap \overline{C} &\Leftrightarrow x \in A \wedge x \in \overline{C} \\ &\Leftrightarrow x \in A \wedge x \notin C \quad (*) \end{aligned}$$

$$\begin{aligned} x \notin A \cap \overline{B} &\Leftrightarrow x \notin A \vee x \notin \overline{B} \\ &\Leftrightarrow x \notin A \vee x \in B. \quad (**) \end{aligned}$$

De (*) sabemos que $x \in A$ e que $x \notin C$. Como $x \in A$, de (**) segue-se que $x \in B$. Assim, x é um objeto tal que $x \in B$ mas $x \notin C$, o que contraria a hipótese de B estar contido em C . Logo, não existem tais conjuntos A, B e C .

5. Diga, justificando, se cada uma das afirmações que se seguem é ou não verdadeira para quaisquer subconjuntos A, B e C não vazios de um conjunto X .

(a) Se $A \subseteq C$ ou $B \subseteq C$ então $A \cup B \subseteq C$.

(b) Se $A \cap B = \emptyset$ então $A \subseteq \overline{B}$.

(c) $(C \setminus A) \cap (A \cup B) = C \setminus B$.

resolução:

(a) Consideremos $A = \{1, 2\}$, $B = \{3, 4\}$ e $C = \{1, 2, 3\}$. Temos que $A \subseteq C$ mas $A \cup B \not\subseteq C$. Logo, a afirmação é falsa.

(b) Admitamos, por redução ao absurdo, que $A \cap B = \emptyset$ e $A \not\subseteq \overline{B}$. De $A \not\subseteq \overline{B}$ segue-se que existe x tal que $x \in A$ e $x \notin \overline{B}$, ou seja, tal que $x \in A$ e $x \in B$. Assim, $x \in A \cap B$, o que contraria o facto $A \cap B = \emptyset$. Portanto, a afirmação é verdadeira.

(c) Consideremos $A = \{1, 2\}$, $B = \{1, 2, 3\}$ e $C = \{1, 2, 3\}$. Temos que

$$(C \setminus A) \cap (A \cup B) = \{3\} \cap \{1, 2, 3\} = \{3\}$$

e

$$C \setminus B = \emptyset.$$

Assim, a afirmação é falsa.

6. Diga, justificando, se cada uma das afirmações que se seguem é ou não verdadeira para quaisquer conjuntos A, B e C .

(a) Se $A \subseteq C$ ou $B \subseteq C$, então $A \cap B \subseteq C$.

(b) Se $(A \times C) \setminus (B \times C) = \emptyset$, então $A \subseteq B$.

(c) Se $A \in B$, então $\mathcal{P}(A) \subseteq \mathcal{P}(B)$.

resolução:

(a) Admitamos que $A \subseteq C$. O caso em que $B \subseteq C$ é análogo. Pretendemos mostrar que todos os elementos de $A \cap B$ são elementos de C . Consideremos um elemento arbitrário x de $A \cap B$. Por definição, $x \in A$ e $x \in B$. Como $A \subseteq C$ e $x \in A$, segue-se que $x \in C$. Assim, se $x \in A \cap B$, então $x \in C$, ou seja, $A \cap B \subseteq C$. A afirmação é, portanto, verdadeira.

(b) Consideremos $A = \{1, 2\}$, $B = \{3, 4\}$ e $C = \emptyset$. Temos que

$$(A \times C) \setminus (B \times C) = \emptyset \setminus \emptyset$$

mas

$$A \not\subseteq B.$$

Logo, a afirmação é falsa.

(c) Sejam $A = \{1\}$ e $B = \{\{1\}, 2\}$. Temos que $A \in B$. No entanto, $\{1\} \in \mathcal{P}(A)$ mas $\{1\} \notin \mathcal{P}(B)$. Logo, $\mathcal{P}(A) \not\subseteq \mathcal{P}(B)$. A afirmação é, pois, falsa.

7. Mostremos que, dados quaisquer três conjuntos A, B e C , se $A \subseteq C$ ou $B \subseteq C$, então $(A \cap B) \subseteq C$.

resolução: Pretendemos mostrar que se $A \subseteq C$ ou $B \subseteq C$, então todos os elementos de $A \cap B$ são elementos de C .

Admitamos que $A \subseteq C$ (o caso em que $B \subseteq C$ é análogo). Por definição, sabemos que, para todo o x , se $x \in A$ então $x \in C$. Mostremos que qualquer elemento de $A \cap B$ é, também, elemento de C . Temos que

$$\begin{aligned} x \in A \cap B &\Leftrightarrow x \in A \wedge x \in B \text{ [pela definição de interseção de conjuntos]} \\ &\Rightarrow x \in A \\ &\Rightarrow x \in C \text{ [porque } A \subseteq C] \end{aligned}$$

Assim, mostramos que $A \cap B \subseteq C$.

8. Sejam A, B e C subconjuntos de um conjunto X . Prove que $(A \setminus B) \setminus (C \setminus B) = A \setminus (B \cup C)$.

resolução: Seja x um elemento arbitrário de X . Temos que

$$\begin{aligned}
x \in (A \setminus B) \setminus (C \setminus B) &\Leftrightarrow x \in (A \setminus B) \wedge x \notin (C \setminus B) \text{ [pela definição de complementação de conjuntos]} \\
&\Leftrightarrow (x \in A \wedge x \notin B) \wedge (x \notin C \vee x \in B) \text{ [pela definição da complementação de conjuntos]} \\
&\Leftrightarrow x \in A \wedge (x \notin B \wedge (x \notin C \vee x \in B)) \text{ [pela associatividade da conjunção]} \\
&\Leftrightarrow x \in A \wedge ((x \notin B \wedge x \notin C) \vee (x \notin B \wedge x \in B)) \text{ [pela distributividade da conjunção} \\
&\hspace{15em} \text{em relação à disjunção]} \\
&\Leftrightarrow x \in A \wedge ((x \notin B \wedge x \notin C) \vee \perp) \text{ [porque } (x \notin B \wedge x \in B) \Leftrightarrow \perp\text{]} \\
&\Leftrightarrow x \in A \wedge (x \notin B \wedge x \notin C) \text{ [porque } \perp \text{ é o elemento neutro para a disjunção]} \\
&\Leftrightarrow x \in A \wedge x \notin (B \cup C) \text{ [pela definição de reunião de conjuntos]} \\
&\Leftrightarrow x \in A \setminus (B \cup C) \text{ [pela definição de complementação de conjuntos]}
\end{aligned}$$

Logo, para todo o x , $x \in (A \setminus B) \setminus (C \setminus B)$ se e só se $x \in A \setminus (B \cup C)$. Assim, podemos concluir que os conjuntos são iguais.

Capítulo 3

Indução nos Naturais

[Exemplo]

Consideremos a afirmação “Para qualquer natural n , $n^2 - n + 41$ é primo”.

Atribuindo valores a n , podemos verificar a veracidade das proposições correspondentes obtidas a partir do predicado $p(n)$: “o número $n^2 - n + 41$ é primo”.

n	1	2	3	4	5	6	...	40	41	...
$n^2 - n + 41$	41	43	47	53	61	71	...	1601	41^2	...

41 é um número primo, pelo que $p(1)$ é verdadeira.

43 é um número primo, pelo que $p(2)$ é verdadeira.

47 é um número primo, pelo que $p(3)$ é verdadeira.

53 é um número primo, pelo que $p(4)$ é verdadeira.

61 é um número primo, pelo que $p(5)$ é verdadeira.

71 é um número primo, pelo que $p(6)$ é verdadeira.

(...)

1601 é um número primo, pelo que $p(40)$ é verdadeira.

Poderemos, assim, concluir que $p(n)$ é verdadeira para todo $n \in \mathbb{N}$?

41^2 não é um número primo, pelo que $p(41)$ é falsa! Portanto, a afirmação “Para qualquer natural n , $n^2 - n + 41$ é primo” é falsa, ao contrário do que poderíamos intuir da veracidade das proposições $p(n)$ com $1 \leq n \leq 40$.

Para provarmos que uma determinada propriedade é válida para todo o número natural, precisamos de um método de prova adequado. Como o exemplo anterior o ilustra, não basta verificar a veracidade da propriedade para um número finito de naturais para podermos concluir a validade da propriedade em \mathbb{N} .

A definição indutiva de \mathbb{N} através das seguintes regras

- i | $1 \in \mathbb{N}$;
- ii | se $n \in \mathbb{N}$, então $n + 1 \in \mathbb{N}$,

justifica a adoção do método de prova que iremos estudar. Começemos por apresentar o conceito de predicado hereditário.

[Definição 3.1] Um predicado $p(n)$, com \mathbb{N} como universo de variação da variável n , diz-se **hereditário** quando, para todo $k \in \mathbb{N}$, se a proposição $p(k)$ é verdadeira, então a proposição $p(k + 1)$ é verdadeira.

[Exemplos]

- 1 | “ $2n$ é par” é um predicado hereditário pois se $2k$ é par para algum $k \in \mathbb{N}$, então $2(k + 1) = 2k + 2$ também é par (por ser a soma de 2 números pares).
- 2 | “ n é par” não é um predicado hereditário pois se k é par para algum $k \in \mathbb{N}$, então $k + 1$ é ímpar.
- 3 | “ $2n + 1$ é par” é um predicado hereditário pois se $2k + 1$ é par para algum $k \in \mathbb{N}$, então $2(k + 1) + 1 = 2k + 2 + 1 = (2k + 1) + 2$ também é par (por ser a soma de 2 números pares).

[Observação] Note-se que, sendo $p(n)$ um predicado hereditário, a proposição $p(a)$, com $a \in \mathbb{N}$, não tem de ser verdadeira. De facto, no terceiro exemplo temos um predicado hereditário $p(n)$ tal que $p(a)$ é uma proposição falsa para qualquer $a \in \mathbb{N}$. Já o predicado $q(n)$ do primeiro exemplo é hereditário e $q(a)$ é uma proposição verdadeira para todo $a \in \mathbb{N}$: é claro que $q(1)$ é verdadeira pois $2 \times 1 = 2$ é par; a hereditariedade de $q(n)$ permite-nos induzir que a propriedade é válida para todo o número natural. Por outro lado, a hereditariedade de $p(n)$ não é suficiente para concluir que a propriedade é verdadeira para todo o número natural, uma vez que nos falta um ponto de partida.

No resultado que se segue encontramos um método de prova usado para demonstrar a veracidade de propriedades sobre os números naturais.

[Teorema 3.2 | princípio de indução (simples) para \mathbb{N}] Seja $p(n)$ um predicado sobre \mathbb{N} . Se

- 1 | $p(1)$ é verdadeira; e
 - 2 | $p(n)$ é hereditário, ou seja, para todo $k \in \mathbb{N}$, se $p(k)$ é verdadeira, então $p(k + 1)$ é verdadeira,
- então $p(n)$ é verdadeira para todo $n \in \mathbb{N}$.

demonstração: Admitamos que as condições 1 | e 2 | são satisfeitas para o predicado $p(n)$ e mostremos que, para qualquer natural n , $p(n)$ é verdadeira. Nesse sentido, consideremos o conjunto X dos números naturais que não satisfazem $p(n)$, ou seja,

$$X = \{n \in \mathbb{N} : \neg p(n)\}.$$

Suponhamos, no intuito de uma redução ao absurdo, que $X \neq \emptyset$. Seja m o menor número natural que pertence a X . Por 1 |, $1 \notin X$ e, portanto, $m > 1$. Logo, $m = k + 1$ para algum $k \in \mathbb{N}$.

Uma vez que m é o menor natural que pertence a X , sabemos que $m - 1 = (k + 1) - 1 = k$ não pertence a X , isto é, k satisfaz o predicado $p(n)$. Ora, por 2 |, $p(n)$ é hereditário e, portanto, $k + 1$ satisfaz o predicado $p(n)$, ou seja, m satisfaz $p(n)$, o que contradiz o facto de m pertencer a X . Logo, X tem de ser vazio e, assim, $p(n)$ é verdadeira para todo $n \in \mathbb{N}$. ■

A condição 1 | do teorema anterior é designada por **base de indução** e a condição 2 | por **passo de indução**.

Na aplicação da condição 2 |, chamamos **hipótese de indução** a “ $p(k)$ é verdadeira”. É habitual usar a sigla H.I. para denotar a hipótese de indução.

Dado um predicado $p(n)$ sobre \mathbb{N} , uma aplicação deste princípio para provar que a proposição $\forall n \, p(n)$ é verdadeira diz-se uma **prova por indução nos naturais**.

[Exemplo]

Mostremos que $n^3 - n$ é divisível por 3, para todo o natural $n \in \mathbb{N}$, pelo método de indução nos naturais.

Representemos por $p(n)$ o predicado “ $n^3 - n$ é divisível por 3”.

1 | base de indução | Para $n = 1$, temos $n^3 - n = 1^3 - 1 = 0$.

Como 0 é divisível por 3, $p(1)$ é verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $p(k)$ é verdadeira, ou seja, $k^3 - k$ é divisível por 3 (H.I.).

Então, existe $q \in \mathbb{N}_0$ tal que $k^3 - k = 3q$. Assim,

$$\begin{aligned} (k+1)^3 - (k+1) &= (k^3 + 3k^2 + 3k + 1) - (k+1) \\ &= k^3 + 3k^2 + 3k - k \\ &= (k^3 - k) + (3k^2 + 3k) \\ &= 3q + (3k^2 + 3k) && \text{(pela H.I.)} \\ &= 3(q + k^2 + k). \end{aligned}$$

Logo, $(k+1)^3 - (k+1) = 3(q + k^2 + k)$, pelo que $p(k+1)$ é verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por 1 | e 2 |, podemos concluir que

$$\forall n \in \mathbb{N} \, n^3 - n \text{ é divisível por 3.}$$

[Exemplo]

Mostremos que a soma dos n primeiros números naturais ímpares é igual a n^2 , para todo o natural $n \in \mathbb{N}$, pelo método de indução nos naturais.

Representemos por $q(n)$ o predicado “ $1 + 3 + 5 + \cdots + (2n - 1) = n^2$ ”.

1 | base de indução | Para $n = 1$, temos $1 = 1^2$, pelo que $q(1)$ é verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $q(k)$ é verdadeira, ou seja, $1 + 3 + 5 + \cdots + (2k - 1) = k^2$ (H.I.). Então,

$$\begin{aligned} 1 + 3 + 5 + \cdots + (2k - 1) + (2(k + 1) - 1) &= (1 + 3 + 5 + \cdots + (2k - 1)) + (2k + 1) \\ &= k^2 + (2k + 1) \\ &= k^2 + 2k + 1 \\ &= (k + 1)^2, \end{aligned} \quad (\text{pela H.I.})$$

pelo que $q(k + 1)$ é verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por 1 | e 2 |, podemos concluir que

$$\forall n \in \mathbb{N}, 1 + 3 + 5 + \cdots + (2n - 1) = n^2.$$

[Exemplo]

Mostremos que, para todo $n \in \mathbb{N}$,

$$\left(1 + \frac{1}{3}\right)^n \geq 1 + \frac{n}{3},$$

pelo método de indução nos naturais.

Representemos por $h(n)$ o predicado “ $\left(1 + \frac{1}{3}\right)^n \geq 1 + \frac{n}{3}$ ”.

1 | base de indução | Para $n = 1$, temos $\left(1 + \frac{1}{3}\right)^1 = 1 + \frac{1}{3} \geq 1 + \frac{1}{3} = 1 + \frac{n}{3}$, pelo que $h(1)$ é verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $h(k)$ é verdadeira, ou seja,

$$\left(1 + \frac{1}{3}\right)^k \geq 1 + \frac{k}{3} \quad (\text{H.I.})$$

Segue-se que

$$\begin{aligned} \left(1 + \frac{1}{3}\right)^{(k+1)} &= \left(1 + \frac{1}{3}\right)^k \left(1 + \frac{1}{3}\right) \\ &\geq \left(1 + \frac{k}{3}\right) \left(1 + \frac{1}{3}\right) \quad (\text{pela H.I.}) \\ &= 1 + \frac{k}{3} + \frac{1}{3} + \frac{k}{9} \\ &= 1 + \frac{k+1}{3} + \frac{k}{9} \\ &\geq 1 + \frac{k+1}{3}. \end{aligned}$$

Assim, $\left(1 + \frac{1}{3}\right)^{(k+1)} \geq 1 + \frac{k+1}{3}$, pelo que $h(k + 1)$ é verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por 1 | e 2 |, podemos concluir que para todo $n \in \mathbb{N}$, $\left(1 + \frac{1}{3}\right)^n \geq 1 + \frac{n}{3}$.

Como já referimos, é necessário que se verifiquem simultaneamente a base e o passo de indução para que se possa induzir a validade da propriedade em causa para todo o número natural.

Consideremos o predicado $p(n)$: “ $n^2 > 2n + 1$ ”.

Facilmente se verifica que $p(1)$ é falsa: $1^2 = 1 \not> 3 = 2 \times 1 + 1$.

No entanto, o passo de indução verifica-se, ou seja, o predicado $p(n)$ é hereditário. Consideremos $k \in \mathbb{N}$ tal que $k^2 > 2k + 1$ (H.I.),

$$\begin{aligned} (k+1)^2 &= k^2 + 2k + 1 \\ &= k^2 + (2k + 1) \\ &> (2k + 1) + (2k + 1) \quad (\text{pela H.I.}) \\ &= 2k + 2 + 2k \\ &> 2k + 2 + 1 \\ &= 2(k+1) + 1. \end{aligned}$$

Na verdade, $p(n)$ é válida para todos os naturais maiores ou iguais a 3.

A prova deste resultado pode ser feita recorrendo a uma variante do Princípio de Indução, considerando para base de indução o elemento de \mathbb{N} a partir do qual se pode provar a validade da propriedade.

[Teorema 3.3 | princípio de indução (simples) para \mathbb{N} de base n_0] Sejam $p(n)$ um predicado sobre \mathbb{N} e $n_0 \in \mathbb{N}$. Se

- 1 | $p(n_0)$ é verdadeira; e
 - 2 | para todo $k \in \mathbb{N}$ tal que $k \geq n_0$, se $p(k)$ é verdadeira, então $p(k+1)$ é verdadeira,
- então $p(n)$ é verdadeira para todo $n \in \mathbb{N}$ tal que $n \geq n_0$.

[Exemplo]

Verifiquemos, então, que para todo $n \geq 3$, $n^2 > 2n + 1$.

1 | base de indução | Para $n = 3$, temos $n^2 = 3^2 = 9 > 7 = 2 \times 3 + 1$, pelo que $p(3)$ é verdadeira.

2 | passo de indução | Mostrámos acima que $p(n)$ é hereditário. Assim, dado $k \in \mathbb{N}$ tal que $k \geq 3$, $p(k+1)$ é verdadeira sempre que $p(k)$ é verdadeira.

Pelo Princípio de Indução para \mathbb{N} de base 3 e por 1 | e 2 |, podemos concluir que para todo $n \geq 3$, $n^2 > 2n + 1$.

[Exemplo]

Mostremos que para todo $n \geq 5$, $2^n > n^2$, pelo método de indução para \mathbb{N} de base 5.

Representemos por $p(n)$ o predicado “ $2^n > n^2$ ”.

1 | base de indução | Para $n = 5$, temos $2^n = 2^5 = 32 > 25 = 5^2$, pelo que $p(5)$ é verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $k \geq 5$ e $p(k)$ é verdadeira, ou seja, $2^k > k^2$.

Então,

$$\begin{aligned} 2^{k+1} &= 2 \times 2^k \\ &> 2 \times k^2 && \text{(pela H.I.)} \\ &= k^2 + k^2 \\ &> k^2 + 2k + 1 && \text{(pelo exemplo anterior)} \\ &= (k+1)^2, \end{aligned}$$

pelo que $p(k+1)$ é verdadeira.

Pelo Princípio de Indução para \mathbb{N} de base 5 e por 1 | e 2 |, podemos concluir que para todo $n \geq 5$, $2^n > n^2$.

Na prova de certas propriedades sobre os naturais, a aplicação do Princípio de Indução Simples não é fácil. Nestes casos, torna-se mais conveniente optar por um outro método de prova, o chamado **Princípio de Indução Completa** (ou **Princípio de Indução Forte**).

[Teorema 3.4 | princípio de indução completa para \mathbb{N}] Seja $p(n)$ um predicado sobre \mathbb{N} . Se

1 | $p(1)$ é verdadeira; e

2 | para todo $k \in \mathbb{N}$, se, para todo $j \in \{1, \dots, k\}$, $p(j)$ é verdadeira, então $p(k+1)$ é verdadeira,

então $p(n)$ é verdadeira para todo $n \in \mathbb{N}$.

Este princípio parece ser mais geral do que o Princípio de Indução Simples, mas prova-se serem equivalentes: toda a prova que possa ser feita pelo Princípio de Indução Simples pode ser feita pelo Princípio de Indução Completa e vice-versa.

À semelhança do que acontece com o Princípio de Indução Simples, podemos enunciar o **Princípio de Indução Completa de base n_0** .

[Teorema 3.5 | princípio de indução completa para \mathbb{N} de base n_0] Sejam $p(n)$ um predicado sobre \mathbb{N} e $n_0 \in \mathbb{N}$. Se

1 | $p(n_0)$ é verdadeira; e

2 | para todo $k \in \mathbb{N}$ tal que $k \geq n_0$, se, para todo $j \in \{n_0, \dots, k\}$, $p(j)$ é verdadeira, então $p(k+1)$ é verdadeira,

então $p(n)$ é verdadeira para todo $n \in \mathbb{N}$ tal que $n \geq n_0$.

[Exemplo]

Recorrendo ao Princípio de Indução Completa de base 2, mostremos que todo o número natural diferente de 1 é primo ou é um produto de números primos.

Representemos por $p(n)$ o predicado “ n é primo ou n é um produto de primos.”.

1 | base de indução | 2 é primo e, portanto, $p(2)$ é verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $k \geq 2$ e admitamos que $p(j)$ é verdadeira para todo $j \in \{2, \dots, k\}$ (H.I.).

Se $k + 1$ é primo, então $p(k + 1)$ é verdadeira.

Se $k + 1$ não é primo, então existem $a, b \in \mathbb{N}$ tais que $1 < a, b < k + 1$ e $k + 1 = ab$.

Pela H.I., como $a, b \in \{2, \dots, k\}$, sabemos que a é primo ou um produto de primos e b é primo ou um produto de primos.

Logo, $k + 1 = ab$ é um produto de primos, pelo que $p(k + 1)$ é verdadeira.

Por 1 | e 2 | e pelo Princípio de Indução Completa de base 2, mostramos que todo o número natural diferente de 1 é primo ou é um produto de primos.

3.1 Exercícios resolvidos

1. Prove, por indução nos naturais, que $2^n \geq 2n$.

resolução: Seja $p(n)$ o predicado $2^n \geq 2n$ sobre $n \in \mathbb{N}$.

1 | base de indução | $2^1 = 2 \geq 2 \times 1$, pelo que $p(1)$ é uma proposição verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $2^k \geq 2k$ (H.I.)

Temos que

$$\begin{aligned} 2^{k+1} &= 2 \times 2^k \\ &\geq 2 \times 2k && \text{(pela H.I.)} \\ &= 2k + 2k \\ &\geq 2k + 2 && \text{(porque } k \geq 1) \\ &= 2(k + 1), \end{aligned}$$

pelo que $p(k + 1)$ é uma proposição verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por 1 | e 2 |, podemos concluir que, para todo $n \in \mathbb{N}$, $2^n \geq 2n$.

2. Prove, por indução nos naturais, que $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}(3^n - 1)$, para todo $n \in \mathbb{N}$.

resolução: Seja $p(n)$ o predicado $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}(3^n - 1)$ sobre $n \in \mathbb{N}$.

1 | base de indução | $3 = \frac{3}{2}(3^1 - 1)$, pelo que $p(1)$ é uma proposição verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $3 + 3^2 + 3^3 + \dots + 3^k = \frac{3}{2}(3^k - 1)$ (H.I.).

Assim

$$\begin{aligned}
3 + 3^2 + 3^3 + \dots + 3^k + 3^{k+1} &= \frac{3}{2}(3^k - 1) + 3^{k+1} && \text{(pela H.I.)} \\
&= \frac{3}{2}3^k - \frac{3}{2} + 3 \times 3^k \\
&= \frac{9}{2}3^k - \frac{3}{2} \\
&= \frac{3}{2}(3 \times 3^k - 1) \\
&= \frac{3}{2}(3^{k+1} - 1),
\end{aligned}$$

pelo que $p(k+1)$ é uma proposição verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por $1 \mid 2$, podemos concluir que, para todo $n \in \mathbb{N}$, $3 + 3^2 + 3^3 + \dots + 3^n = \frac{3}{2}(3^n - 1)$.

3. Mostre que $4^n + 15n - 1$ é múltiplo de 9 para todo o natural n .

resolução: Seja $p(n)$ o predicado “ $4^n + 15n - 1$ é múltiplo de 9” sobre $n \in \mathbb{N}$.

1 | base de indução | $4^1 + 15 \times 1 - 1 = 18$, que é múltiplo de 9. Logo, $p(1)$ é uma proposição verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $p(k)$ é verdadeira, isto é, $4^k + 15k - 1$ é múltiplo de 9. Assim, existe $q \in \mathbb{Z}$ tal que $4^k + 15k - 1 = 9q$ (H.I.).

Temos que

$$\begin{aligned}
4^{k+1} + 15(k+1) - 1 &= 4 \times 4^k + 15k + 15 - 1 \\
&= (4 \times 4^k + 4 \times 15k - 4) - 3 \times 15k + 15 + 3 \\
&= 4 \times (4^k + 15k - 1) - 3 \times 15k + 18 \\
&= 4 \times 9q - 9 \times 5k + 9 \times 2 && \text{(pela H.I.)} \\
&= 9 \times (4q - 5k + 2),
\end{aligned}$$

que é múltiplo de 9. Portanto, $p(k+1)$ é uma proposição verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por $1 \mid 2$, podemos concluir que, para todo $n \in \mathbb{N}$, $4^n + 15n - 1$ é múltiplo de 9.

4. Mostre que $n^2 - 1$ é divisível por 8 para todo o natural ímpar n .

resolução: Note-se que mostrar que $n^2 - 1$ é divisível por 8 para todo o natural ímpar n é o mesmo que mostrar que $(2m - 1)^2 - 1$ é divisível por 8 para todo o natural m , uma vez que um natural n é ímpar se e só se existe $m \in \mathbb{N}$ tal que $n = 2m - 1$.

Seja $p(m)$ o predicado “ $(2m - 1)^2 - 1$ é divisível por 8” sobre os naturais m .

1 | base de indução | $(2 \times 1 - 1)^2 - 1 = 0$, que é divisível por 8. Logo, $p(1)$ é uma proposição verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $p(k)$ é verdadeira, isto é, $(2k-1)^2 - 1$ é divisível por 8. Assim, existe $q \in \mathbb{Z}$ tal que $(2k-1)^2 - 1 = 8q$

Temos que

$$\begin{aligned}
 (2(k+1)-1)^2 - 1 &= ((2k-1)+2)^2 - 1 \\
 &= (2k-1)^2 + 2 \times 2 \times (2k-1) + 2^2 - 1 \\
 &= ((2k-1)^2 - 1) + 4(2k-1) + 4 \\
 &= 8q + 8k \\
 &= 8 \times (q+k), \quad \text{(pela H.I.)}
 \end{aligned}$$

pelo que $(2(k+1)-1)^2 - 1$ é divisível por 8 e, por conseguinte, $p(k+1)$ é uma proposição verdadeira.

Pelo Princípio de Indução para \mathbb{N} e por $1 \mid 2$, podemos concluir que, para todo $n \in \mathbb{N}$, $(2n-1)^2 - 1$ é divisível por 8. Equivalentemente, podemos concluir que $n^2 - 1$ é divisível por 8 para todo o natural ímpar n .

5. Os números de Fibonacci estão definidos de seguinte forma: $f_1 = f_2 = 1$ e, se $n > 2$, $f_n = f_{n-1} + f_{n-2}$. Prove que $2^{n-1} > f_n > (\frac{3}{2})^{n-1}$ para todo $n \geq 6$.

resolução: Seja $p(n)$ o predicado $2^{n-1} > f_n > (\frac{3}{2})^{n-1}$ sobre os naturais $n \geq 6$.

1 | base de indução | $2^5 = 32 > 8 = f_6 > \frac{243}{32} = (\frac{3}{2})^5$, pelo que $p(6)$ é uma proposição verdadeira.

2 | passo de indução | Seja $k \in \mathbb{N}$ tal que $k \geq 6$ e $p(6), \dots, p(k)$ são proposições verdadeiras (H.I.), ou seja, $2^5 > f_6 > (\frac{3}{2})^5, \dots, 2^{k-2} > f_{k-1} > (\frac{3}{2})^{k-2}, 2^{k-1} > f_k > (\frac{3}{2})^{k-1}$.

Então,

$$\begin{aligned}
 f_{k+1} = f_k + f_{k-1} &< 2^{k-1} + 2^{k-2} \quad \text{(pela H.I.)} \\
 &= 2 \times 2^{k-2} + 2^{k-2} \\
 &= (2+1) \times 2^{k-2} \\
 &= 3 \times 2^{k-2} \\
 &< 4 \times 2^{k-2} \\
 &= 2^2 \times 2^{k-2} \\
 &= 2^k
 \end{aligned}$$

e

$$\begin{aligned}
 f_{k+1} = f_k + f_{k-1} &> (\frac{3}{2})^{k-1} + (\frac{3}{2})^{k-2} \quad \text{(pela H.I.)} \\
 &> (\frac{3}{2})^k,
 \end{aligned}$$

uma vez que

$$\begin{aligned}
\left(\frac{3}{2}\right)^{k-1} + \left(\frac{3}{2}\right)^{k-2} > \left(\frac{3}{2}\right)^k &\Leftrightarrow \frac{3}{2}\left(\frac{3}{2}\right)^{k-2} + \left(\frac{3}{2}\right)^{k-2} > \left(\frac{3}{2}\right)^2\left(\frac{3}{2}\right)^{k-2} \\
&\Leftrightarrow \frac{3}{2} + 1 > \left(\frac{3}{2}\right)^2 \\
&\Leftrightarrow \frac{5}{2} > \frac{9}{4} \\
&\Leftrightarrow 20 > 18,
\end{aligned}$$

o que é uma afirmação verdadeira.

Assim, $2^k > f_{k+1} > \left(\frac{3}{2}\right)^k$, ou seja $p(k+1)$ é uma proposição verdadeira.

Pelo Princípio de Indução Completa para \mathbb{N} de base 6 e por $1 \mid$ e $2 \mid$, podemos concluir que $2^{n-1} > f_n > \left(\frac{3}{2}\right)^{n-1}$ para todo $n \geq 6$.

Capítulo 4

Funções

4.1 Conceitos básicos

[Definição 4.1] Sejam A e B conjuntos. Uma **função** ou **aplicação** de A em B é uma correspondência de A para B que a cada elemento de A faz corresponder um e um só elemento de B .

Em geral, representamos as funções por letras minúsculas f, g, h, \dots

Escrevemos $f : A \rightarrow B$ para indicar que f é uma função de A em B . Para cada objeto $a \in A$, o único elemento b de B que f faz corresponder ao elemento a chama-se **imagem de a por f** e representa-se por $f(a)$. Podemos, assim, escrever

$$\begin{aligned} f : A &\rightarrow B \\ a &\mapsto f(a) \end{aligned}$$

Dada uma função $f : A \rightarrow B$, designamos por

- 1 | **domínio** ou **conjunto de partida** de f o conjunto A ;
- 2 | **codomínio** ou **conjunto de chegada** de f o conjunto B ;
- 3 | **imagem** ou **contradomínio** de f o conjunto $\text{Im}(f)$ das imagens por f de todos os elementos de A , ou seja,

$$\text{Im}(f) = \{f(x) : x \in A\}.$$

O conjunto de todas as funções de A para B representa-se por B^A .

Dado um conjunto A , chama-se **aplicação vazia** à aplicação $\emptyset : \emptyset \rightarrow A$. Esta é a única aplicação de \emptyset em A e, portanto, $A^\emptyset = \{\emptyset\}$.

Se A é não vazio, não existem funções de A em \emptyset , pelo que $\emptyset^A = \emptyset$.

Se A e B são conjuntos finitos, temos que $\#B^A = (\#B)^{\#A}$.

[Exemplos]

[1] A correspondência de \mathbb{Z} em \mathbb{Z} que a cada elemento x de \mathbb{Z} faz corresponder o elemento $y = x^2$ é uma função de \mathbb{Z} em \mathbb{Z} .

[2] Seja $A = \{1, 2, 3\}$ e sejam f, g, h e ℓ as correspondências definidas por

$$\begin{array}{llll} f: A \rightarrow A & g: A \rightarrow A & h: A \rightarrow A & \ell: A \rightarrow A \\ 1 \mapsto 2 & 1 \mapsto 2 & 1 \mapsto 1 & 1 \mapsto 1 \\ 2 \mapsto 1 & 2 \mapsto 2 & 1 \mapsto 2 & 2 \mapsto 2 \\ 3 \mapsto 3 & 3 \mapsto 2 & 2 \mapsto 2 & 3 \mapsto 3 \\ & & 3 \mapsto 3 & \end{array} .$$

Então, f e g são funções de A em A . Por outro lado, h não é uma função de A em A uma vez que a 1 faz corresponder duas imagens: 1 e 2. Também ℓ não é uma função de A em A uma vez que a 2 não faz corresponder qualquer imagem.

[3] Sejam A e B conjuntos, com $B \neq \emptyset$. Seja $b \in B$. A correspondência de A em B que a cada elemento de A faz corresponder o elemento b é uma função de A em B .

[Definição 4.2] Sejam A e B conjuntos. Uma função $f: A \rightarrow B$ diz-se uma **função constante** se existe $b \in B$ tal que, para todo o $a \in A$, $f(a) = b$.

A função de A em A que a cada elemento $a \in A$ faz corresponder a diz-se a **função identidade de A** e representa-se por id_A , ou seja,

$$\begin{array}{l} \text{id}_A: A \rightarrow A \\ a \mapsto a \end{array}$$

[Exemplo]

Sejam $A = \{1, 2, 3\}$ e $B = \{4, 5\}$. Então,

$$\begin{array}{l} \text{id}_A: A \rightarrow A \\ 1 \mapsto 1 \\ 2 \mapsto 2 \\ 3 \mapsto 3 \\ \text{id}_B: B \rightarrow B \\ 4 \mapsto 4 \\ 5 \mapsto 5 \end{array}$$

e a correspondência

$$\begin{array}{l} f: A \rightarrow B \\ 1 \mapsto 4 \\ 2 \mapsto 4 \\ 3 \mapsto 4 \end{array}$$

é uma função constante.

[Definição 4.3] Sejam A_1, A_2, B_1, B_2 conjuntos e sejam $f : A_1 \rightarrow B_1$, $g : A_2 \rightarrow B_2$ funções. Dizemos que as funções f e g são **iguais**, e escrevemos $f = g$, se

- 1 | $A_1 = A_2$;
- 2 | $B_1 = B_2$;
- 3 | para todo o $x \in A_1$, $f(x) = g(x)$.

[Exemplo]

Sejam $f : \mathbb{Z} \rightarrow \mathbb{Z}$, $g : \mathbb{Z} \rightarrow \mathbb{Z}$, $h : \mathbb{Q} \rightarrow \mathbb{R}$ e $k : \mathbb{Q} \rightarrow \mathbb{Q}$ funções definidas, respetivamente, por

$$f(x) = \begin{cases} x, & \text{se } x \geq 0 \\ -x & \text{se } x < 0 \end{cases}, \quad g(x) = |x|, \forall x \in \mathbb{Z}, \quad h(x) = k(x) = |x|, \forall x \in \mathbb{Q}.$$

Como os domínios de g e de h são distintos, $g \neq h$. De igual modo, $g \neq k$. Como os codomínios de h e de k são distintos, $h \neq k$. Por outro lado, como os domínios e os codomínios de f e g são iguais e $f(x) = g(x)$ para todo o $x \in \mathbb{Z}$, podemos concluir que $f = g$.

4.2 Conjuntos Imagem e Imagem Inversa

[Definição 4.4] Sejam A, B conjuntos, X um subconjunto de A , Y um subconjunto de B e $f : A \rightarrow B$ uma função de A em B . Designamos por

- 1 | **imagem de X por f** o conjunto

$$f(X) = \{f(x) : x \in X\};$$

- 2 | **imagem inversa ou pré-imagem de Y por f** o conjunto

$$f^{\leftarrow}(Y) = \{x \in A : f(x) \in Y\}.$$

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6\}$ e $f : A \rightarrow B$ a função definida por $f(1) = f(2) = 4$ e $f(3) = 5$.

Então, $f(\{1, 2\}) = \{f(1), f(2)\} = \{4, 4\} = \{4\}$, $f^{\leftarrow}(\{4, 5\}) = \{1, 2, 3\} = A$ e $f^{\leftarrow}(\{6\}) = \emptyset$.

[2] Sejam $f : \mathbb{Z} \rightarrow \mathbb{Z}$ a aplicação definida por

$$f(x) = \begin{cases} 2x + 3 & \text{se } x \geq 0 \\ 3 - x & \text{se } x < 0 \end{cases},$$

$X = \{-4, 0, 1, 2\}$ e $Y = \{-5, 0, 5\}$. Então,

$$f(X) = \{f(-4), f(0), f(1), f(2)\} = \{7, 3, 5, 7\} = \{3, 5, 7\}$$

$$\begin{aligned}
f^{\leftarrow}(Y) &= \{x \in \mathbb{Z} : f(x) = -5 \vee f(x) = 0 \vee f(x) = 5\} \\
&= \{x \in \mathbb{Z} : (2x + 3 = -5 \wedge x \geq 0) \vee (3 - x = -5 \wedge x < 0) \vee \\
&\quad \vee (2x + 3 = 0 \wedge x \geq 0) \vee (3 - x = 0 \wedge x < 0) \vee \\
&\quad \vee (2x + 3 = 5 \wedge x \geq 0) \vee (3 - x = 5 \wedge x < 0)\} \\
&= \{1, -2\}
\end{aligned}$$

[3] Consideremos a função

$$\begin{aligned}
f : \mathbb{R} &\rightarrow \mathbb{R} \\
x &\mapsto |x|
\end{aligned}$$

Então,

$$i \mid f(\{-1, 0, 1\}) = \{0, 1\}; f(\mathbb{R}) = \mathbb{R}_0^+; f([-2, 3]) = [0, 3];$$

$$ii \mid f^{\leftarrow}(\{1\}) = \{-1, 1\}; f^{\leftarrow}(\mathbb{R}^-) = \emptyset; f^{\leftarrow}(\mathbb{R}) = \mathbb{R}; f^{\leftarrow}(\mathbb{R}^+) = \mathbb{R}/\{0\}.$$

[Proposição 4.5] Sejam A, B conjuntos, $f : A \rightarrow B$ uma função, $A_1, A_2 \subseteq A$ e $B_1, B_2 \subseteq B$. Então,

$$1 \mid f(\emptyset) = \emptyset;$$

$$2 \mid f(A) \subseteq B;$$

$$3 \mid \text{se } A_1 \subseteq A_2, \text{ então } f(A_1) \subseteq f(A_2);$$

$$4 \mid f(A_1 \cup A_2) = f(A_1) \cup f(A_2);$$

$$5 \mid f^{\leftarrow}(\emptyset) = \emptyset;$$

$$6 \mid f^{\leftarrow}(B) = A;$$

$$7 \mid \text{Se } B_1 \subseteq B_2, \text{ então } f^{\leftarrow}(B_1) \subseteq f^{\leftarrow}(B_2);$$

$$8 \mid f^{\leftarrow}(B_1 \cup B_2) = f^{\leftarrow}(B_1) \cup f^{\leftarrow}(B_2);$$

$$9 \mid f^{\leftarrow}(B_1 \cap B_2) = f^{\leftarrow}(B_1) \cap f^{\leftarrow}(B_2);$$

demonstração:

Iremos demonstrar as propriedades 1, 3, 4, 7 e 8. As restantes são deixadas como exercício.

1 | Por definição, $f(\emptyset) = \{f(x) : x \in \emptyset\}$. Ora, \emptyset não tem elementos, pelo que $x \in \emptyset$ é uma condição impossível. Portanto, $f(\emptyset) = \emptyset$.

3 | Suponhamos que $A_1 \subseteq A_2$. Então, para todo o objeto x , se $x \in A_1$ então $x \in A_2$.

Pretendemos mostrar que $f(A_1) \subseteq f(A_2)$, ou seja, para todo o objeto y , se $y \in f(A_1)$ então $y \in f(A_2)$.

Seja $y \in f(A_1)$. Então, existe $x \in A_1$ tal que $y = f(x)$.

Por hipótese, se $x \in A_1$ então $x \in A_2$. Logo, $x \in A_2$ e, assim, $y = f(x)$ com $x \in A_2$. Portanto, $y \in f(A_2)$.

Vimos, então, que se $y \in f(A_1)$ então $y \in f(A_2)$, pelo que $f(A_1) \subseteq f(A_2)$.

4 | Pretendemos mostrar que $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

(\subseteq) Começemos por mostrar que $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$.

Seja $y \in f(A_1 \cup A_2)$. Então, existe $x \in A_1 \cup A_2$ tal que $y = f(x)$.

Ora,

$$x \in A_1 \cup A_2 \Leftrightarrow (x \in A_1 \vee x \in A_2).$$

Se $x \in A_1$, então $y = f(x) \in f(A_1)$. Se $x \in A_2$, então $y = f(x) \in f(A_2)$.

Logo, $y \in f(A_1) \vee y \in f(A_2)$ e, portanto, $y \in f(A_1) \cup f(A_2)$.

(\supseteq) Mostremos, agora, que $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$.

Seja $y \in f(A_1) \cup f(A_2)$. Então, $y \in f(A_1) \vee y \in f(A_2)$. Se $y \in f(A_1)$, então existe $x \in A_1$ tal que $y = f(x)$. Se $y \in f(A_2)$, então existe $x \in A_2$ tal que $y = f(x)$. Em ambos os casos, $x \in A_1 \cup A_2$, pelo que $y = f(x) \in f(A_1 \cup A_2)$.

Logo, $f(A_1 \cup A_2) \subseteq f(A_1) \cup f(A_2)$ e $f(A_1) \cup f(A_2) \subseteq f(A_1 \cup A_2)$, pelo que $f(A_1 \cup A_2) = f(A_1) \cup f(A_2)$.

7 | Suponhamos que $B_1 \subseteq B_2$, ou seja, para todo o objeto y , se $y \in B_1$ então $y \in B_2$.

Queremos mostrar que $f^{\leftarrow}(B_1) \subseteq f^{\leftarrow}(B_2)$. Dado $x \in f^{\leftarrow}(B_1)$, sabemos que $x \in A$ e $f(x) \in B_1$, por definição de imagem inversa. Ora, $B_1 \subseteq B_2$, pelo que $f(x) \in B_2$. Assim, $x \in f^{\leftarrow}(B_2)$.

8 | Verifiquemos, agora, que $f^{\leftarrow}(B_1 \cup B_2) = f^{\leftarrow}(B_1) \cup f^{\leftarrow}(B_2)$.

Dado $x \in A$,

$$\begin{aligned} x \in f^{\leftarrow}(B_1 \cup B_2) &\Leftrightarrow f(x) \in B_1 \cup B_2 \\ &\Leftrightarrow (f(x) \in B_1 \vee f(x) \in B_2) \\ &\Leftrightarrow (x \in f^{\leftarrow}(B_1) \vee x \in f^{\leftarrow}(B_2)) \\ &\Leftrightarrow x \in f^{\leftarrow}(B_1) \cup f^{\leftarrow}(B_2) \end{aligned}$$

Logo, para todo o objeto x , $x \in f^{\leftarrow}(B_1 \cup B_2)$ se e só se $x \in f^{\leftarrow}(B_1) \cup f^{\leftarrow}(B_2)$, donde segue a igualdade pretendida. ■

4.3 Propriedades das funções

[Definição 4.6] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função. Diz-se que f é **injetiva** quando quaisquer dois elementos distintos de A têm imagens distintas por f , ou seja, quando $\forall_{x,y \in A} (x \neq y \Rightarrow f(x) \neq f(y))$. Equivalentemente, f é injetiva quando

$$\forall_{x,y \in A} (f(x) = f(y) \Rightarrow x = y).$$

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$ e $B = \{4, 5, 6, 7\}$ e seja $f : A \rightarrow B$ a função definida por $f(1) = 6$, $f(2) = 7$ e $f(3) = 4$. Então, f é injetiva pois não existem objetos distintos com a mesma imagem.

[2] Sejam $C = \{1, 2, 3, 4\}$ e $D = \{5, 6, 7\}$ e seja $g : C \rightarrow D$ a função definida por $g(1) = 5$, $g(2) = 6$, $g(3) = 7$ e $g(4) = 7$. Então, g não é injetiva pois $3 \neq 4$ e $g(3) = 7 = g(4)$.

[3] Seja $h : \mathbb{Z} \rightarrow \mathbb{Z}$ a função definida por $h(n) = 2n + 1$ para todo o $n \in \mathbb{Z}$. A função h é injetiva pois, dados $n, m \in \mathbb{Z}$,

$$h(n) = h(m) \Leftrightarrow 2n + 1 = 2m + 1 \Leftrightarrow 2n = 2m \Leftrightarrow n = m.$$

[4] Seja $k : \mathbb{R} \rightarrow \mathbb{R}$ a função definida por $k(x) = x^2$, para todo o $x \in \mathbb{R}$. A função k não é injetiva pois $-2 \neq 2$ e $k(-2) = 4 = k(2)$.

[Definição 4.7] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função. Diz-se que f é **sobrejetiva** quando todo o elemento de B é imagem de algum elemento de A , ou seja, quando

$$\forall y \in B \exists x \in A \ f(x) = y.$$

Equivalentemente, f é sobrejetiva se $f(A) = B$, ou seja se o contradomínio coincide com o conjunto de chegada.

[Exemplos]

Consideremos as funções definidas no exemplo anterior.

[1] A função $f : \{1, 2, 3\} \rightarrow \{4, 5, 6, 7\}$ definida por $f(1) = 6$, $f(2) = 7$ e $f(3) = 4$ não é sobrejetiva pois 5 não é imagem de qualquer elemento de A .

[2] A função $g : \{1, 2, 3, 4\} \rightarrow \{5, 6, 7\}$ definida por $g(1) = 5$, $g(2) = 6$, $g(3) = 7$ e $g(4) = 7$ é sobrejetiva pois todo o elemento de $\{5, 6, 7\}$ é imagem de algum elemento de A .

[3] A função $h : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $h(n) = 2n + 1$ para todo o $n \in \mathbb{Z}$, não é sobrejetiva pois, dado $m \in \mathbb{Z}$ par, m não é da forma $2n + 1$, com $n \in \mathbb{N}$. Por conseguinte, não existe, por exemplo, nenhum objeto que tenha imagem igual a 6.

[4] A função $k : \mathbb{R} \rightarrow \mathbb{R}$ definida por $k(x) = x^2$, para todo o $x \in \mathbb{R}$, não é sobrejetiva pois $k(\mathbb{R}) = \mathbb{R}_0^+$. Portanto, não existe, por exemplo, nenhum objeto que tenha imagem igual a -1 .

[Definição 4.8] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função. Diz-se que f é **bijetiva** quando f é injetiva e sobrejetiva, ou equivalentemente, quando

$$\forall y \in B \exists^1 x \in A \ f(x) = y.$$

[Exemplos]

1 | A função $f : \{1, 2, 3\} \rightarrow \{4, 5, 6\}$ definida por $f(1) = 5$, $f(2) = 4$ e $f(3) = 6$ é bijetiva, uma vez que elementos distintos têm imagens distintas e todo o elemento do conjunto de chegada é imagem de algum objeto do domínio.

2 | A função $g : \mathbb{Z} \rightarrow \mathbb{Z}$ definida por $g(n) = n + 1$, para todo o $n \in \mathbb{Z}$ é bijetiva. De facto, dados $n, m \in \mathbb{Z}$

$$g(n) = g(m) \Leftrightarrow n + 1 = m + 1 \Leftrightarrow n = m.$$

Portanto, g é injetiva. Por outro lado, dado $m \in \mathbb{Z}$, $n = m - 1 \in \mathbb{Z}$ e

$$g(n) = g(m - 1) = (m - 1) + 1 = m,$$

pelo que g é sobrejetiva. Como g é injetiva e sobrejetiva, podemos concluir que é bijetiva.

4.4 Função composta

É possível definir novas funções a partir de funções dadas.

[Proposição 4.9] Sejam A, B, C conjuntos e $f : A \rightarrow B$, $g : B \rightarrow C$ funções. Então, a correspondência de A para C que a cada elemento x de A faz corresponder o elemento $g(f(x))$ de C é uma função de A para C .

demonstração:

Como f é uma função de A para B , dado $x \in A$, existe um único elemento y em B tal que $f(x) = y$. Por sua vez, como g é uma função de B para C e y é um elemento de B , existe um único elemento z de C tal que $g(y) = z$.

Assim, para cada elemento x de A , existe um único elemento z de C tal que $g(f(x)) = g(y) = z$. Logo, a correspondência em causa é uma função. ■

[Definição 4.10] Sejam A, B, C conjuntos e $f : A \rightarrow B$, $g : B \rightarrow C$ funções. Designa-se por **função composta de g com f** , e representa-se por $g \circ f$, a função de A para C que a cada elemento x de A faz corresponder o elemento $g(f(x))$ de C , ou seja, $g \circ f$ é a função

$$\begin{aligned} g \circ f : A &\rightarrow C \\ x &\mapsto g(f(x)). \end{aligned}$$

[Exemplos]

[1] Sejam $A = \{1, 2, 3\}$, $B = \{4, 5, 6, 7\}$ e $C = \{8, 9\}$ conjuntos e sejam $f : A \rightarrow B$ e $g : B \rightarrow C$ as funções definidas por $f(1) = 4$, $f(2) = 6$ e $f(3) = 7$ e $g(4) = g(6) = 8$, $g(5) = g(7) = 9$. Então, a função $g \circ f : A \rightarrow C$ define-se da seguinte forma:

$$\begin{aligned}(g \circ f)(1) &= g(f(1)) = g(4) = 8 \\ (g \circ f)(2) &= g(f(2)) = g(6) = 8 \\ (g \circ f)(3) &= g(f(3)) = g(7) = 9\end{aligned}$$

[2] Dadas as funções $f : \mathbb{Z} \rightarrow \mathbb{N}_0$ e $g : \mathbb{N}_0 \rightarrow \mathbb{Z}$ definidas por

$$f(x) = \begin{cases} 2x, & \text{se } x > 0 \\ -3x, & \text{se } x \leq 0 \end{cases} \quad \text{e} \quad g(x) = -x^2, \text{ para todo } x \in \mathbb{N}_0,$$

podemos considerar as funções $g \circ f : \mathbb{Z} \rightarrow \mathbb{Z}$ e $f \circ g : \mathbb{N}_0 \rightarrow \mathbb{N}_0$ definidas por

$$(g \circ f)(x) = \begin{cases} -4x^2, & \text{se } x > 0 \\ -9x^2, & \text{se } x \leq 0 \end{cases} \quad \text{e} \quad (f \circ g)(x) = 3x^2, \text{ para todo } x \in \mathbb{N}_0.$$

Como podemos verificar no exemplo anterior, a composição de funções não é, em geral, comutativa. Prova-se, no entanto, ser válida a propriedade associativa para a composição de funções.

[Proposição 4.11] Sejam A, B, C, D conjuntos e $f : A \rightarrow B$, $g : B \rightarrow C$ e $h : C \rightarrow D$ funções. Então,

$$(h \circ g) \circ f = h \circ (g \circ f).$$

demonstração:

Por definição de função composta, as funções $(h \circ g) \circ f$ e $h \circ (g \circ f)$ têm A como conjunto de partida e D como conjunto de chegada. Além disso, dado $x \in A$,

$$\begin{aligned}((h \circ g) \circ f)(x) &= (h \circ g)(f(x)) \\ &= h(g(f(x))) \\ &= h((g \circ f)(x)) \\ &= (h \circ (g \circ f))(x).\end{aligned}$$

Podemos, pois, concluir que $(h \circ g) \circ f = h \circ (g \circ f)$. ■

A composição de uma função com a função identidade é descrita no resultado que se segue.

[Proposição 4.12] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função. Então, $\text{id}_B \circ f = f = f \circ \text{id}_A$.

demonstração:

Por definição de função composta, as funções $\text{id}_B \circ f$, f e $f \circ \text{id}_A$ têm A como conjunto de partida e B como conjunto de chegada. Além disso, dado $x \in A$,

$$\begin{aligned}(\text{id}_B \circ f)(x) &= \text{id}_B(f(x)) \\ &= f(x)\end{aligned}$$

e

$$\begin{aligned}(f \circ \text{id}_A)(x) &= f(\text{id}_A(x)) \\ &= f(x)\end{aligned}$$

pelo que $(\text{id}_B \circ f)(x) = f(x) = (f \circ \text{id}_A)(x)$.

Assim, podemos afirmar que as funções $\text{id}_B \circ f$, f e $f \circ \text{id}_A$ são iguais. ■

A composição preserva certas propriedades das funções, como podemos comprovar no seguinte resultado.

[Proposição 4.13] Sejam A, B, C conjuntos e $f : A \rightarrow B, g : B \rightarrow C$ funções. Então,

1 | Se f e g são injetivas, então $g \circ f$ é injetiva.

2 | Se f e g são sobrejetivas, então $g \circ f$ é sobrejetiva.

3 | Se f e g são bijetivas, então $g \circ f$ é bijetiva.

demonstração:

1 | Suponhamos que f e g são injetivas. Então, dados $x, y \in A$,

$$\begin{aligned} (g \circ f)(x) = (g \circ f)(y) &\Leftrightarrow g(f(x)) = g(f(y)) \\ &\Rightarrow f(x) = f(y) && (g \text{ é injetiva}) \\ &\Rightarrow x = y && (f \text{ é injetiva}). \end{aligned}$$

Logo, $g \circ f$ é injetiva.

2 | Suponhamos agora que f e g são sobrejetivas. Seja $z \in C$. Como $g : B \rightarrow C$ é sobrejetiva, existe $y \in B$ tal que $z = g(y)$. Ora, $y \in B$ e $f : A \rightarrow B$ é sobrejetiva. Logo, existe $x \in A$ tal que $y = f(x)$.

Assim, existe $x \in A$ tal que

$$z = g(y) = g(f(x)) = (g \circ f)(x).$$

Mostramos que, para todo $z \in C$, existe $x \in A$ tal que $z = (g \circ f)(x)$, ou seja, $g \circ f$ é sobrejetiva.

3 | Suponhamos que f e g são bijetivas. Então, f e g são injetivas e, por 1|, $g \circ f$ também o é. Mais, f e g são sobrejetivas e, por 2|, $g \circ f$ também o é. Logo, $g \circ f$ é bijetiva. ■

4.5 Funções invertíveis

[Teorema 4.14] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função. Então, f é bijetiva se e só se existe uma única função $g : B \rightarrow A$ tal que $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$.

demonstração:

Suponhamos que existe uma tal função g e mostremos que f é bijetiva.

Sejam $x_1, x_2 \in A$ tais que $f(x_1) = f(x_2)$. Então, sendo g uma função, $g(f(x_1)) = g(f(x_2))$, ou seja, $(g \circ f)(x_1) = (g \circ f)(x_2)$. Ora, $(g \circ f)(x_1) = \text{id}_A(x_1) = x_1$ e $(g \circ f)(x_2) = \text{id}_A(x_2) = x_2$. Logo, $x_1 = x_2$. Provamos, assim, que f é injetiva.

Consideremos, agora, $y \in B$. Temos que $y = \text{id}_B(y) = (f \circ g)(y) = f(g(y))$. Como g é função, $g(y) \in A$. Assim, existe $x \in A$ tal que $y = f(x)$: com efeito, basta tomar $x = g(y)$. Podemos, então, afirmar que f é sobrejetiva.

Sendo f injetiva e sobrejetiva, f é bijetiva.

Reciprocamente, admitamos que f é bijetiva e mostremos que existe uma única função g como descrita no enunciado. Consideremos a correspondência $g : B \rightarrow A$ que a cada $b \in B$ faz corresponder o único elemento $a \in A$ tal que $f(a) = b$. Note-se que a existência e unicidade de a são garantidas pelo facto de f ser bijetiva. A correspondência g é, assim, uma função. Para cada $a \in A$, $(g \circ f)(a) = g(f(a)) = a = \text{id}_A(a)$ e, para cada $b \in B$, $(f \circ g)(b) = f(g(b)) = f(a)$, onde a é o único elemento de A tal que $f(a) = b$. Assim, para cada $b \in B$, $(f \circ g)(b) = b = \text{id}_B(b)$. Mostrámos, deste modo, que existe pelo menos uma função g como no enunciado.

Vejam, agora, que tal função é única. Para tal, consideremos $g, h : B \rightarrow A$ funções tais que $g \circ f = \text{id}_A$, $f \circ g = \text{id}_B$, $h \circ f = \text{id}_A$ e $f \circ h = \text{id}_B$. Então,

$$\begin{aligned} g &= \text{id}_A \circ g \\ &= (h \circ f) \circ g \\ &= h \circ (f \circ g) \\ &= h \circ \text{id}_B \\ &= h. \end{aligned}$$

■

[Definição 4.15] Sejam A, B conjuntos e $f : A \rightarrow B$ uma função bijetiva. À única função $g : B \rightarrow A$ tal que $g \circ f = \text{id}_A$ e $f \circ g = \text{id}_B$ chamamos **função inversa de f** . Escrevemos $g = f^{-1}$ e dizemos que **f é invertível**.

[Proposição 4.16] Sejam A, B conjuntos e $f : A \rightarrow B$, $g : B \rightarrow C$ funções bijetivas. Então,

$$1 \mid (f^{-1})^{-1} = f.$$

$$2 \mid (g \circ f)^{-1} = f^{-1} \circ g^{-1}.$$

demonstração:

1 | Pelo teorema 4.13, como f é bijetiva, sabemos que f é invertível, ou seja, existe $f^{-1} : B \rightarrow A$ tal que $f \circ f^{-1} = \text{id}_B$ e $f^{-1} \circ f = \text{id}_A$. Daqui, novamente pelo teorema 4.13, f^{-1} é invertível e $(f^{-1})^{-1} = f$.

2 | Pela proposição 4.12, como f e g são bijetivas, também $g \circ f$ o é, sendo $(g \circ f)^{-1}$ uma função de C em A .

Por outro lado, f^{-1} é uma função de B em A e g^{-1} é uma função de C em B , pelo que $f^{-1} \circ g^{-1}$ é também uma função de C em A .

Além disso, dado $x \in C$, atendendo à proposição 4.11,

$$\begin{aligned}
(f^{-1} \circ g^{-1})(x) &= ((f^{-1} \circ g^{-1}) \circ \text{id}_C)(x) \\
&= ((f^{-1} \circ g^{-1}) \circ (g \circ f) \circ (g \circ f)^{-1})(x) \\
&= (f^{-1} \circ (g^{-1} \circ g) \circ f \circ (g \circ f)^{-1})(x) \\
&= (f^{-1} \circ \text{id}_B \circ f \circ (g \circ f)^{-1})(x) \\
&= (f^{-1} \circ f \circ (g \circ f)^{-1})(x) \\
&= (\text{id}_A \circ (g \circ f)^{-1})(x) \\
&= (g \circ f)^{-1}(x).
\end{aligned}$$

Portanto, as funções $f^{-1} \circ g^{-1}$ e $(g \circ f)^{-1}$ são iguais. ■

4.6 Exercícios resolvidos

1. Sejam $A = \{x \in \mathbb{N} \mid x \geq 8 \text{ e } x \text{ é par}\}$, $f : \mathbb{N} \rightarrow A$, $h : \mathbb{N} \rightarrow \mathbb{N}$ e $g : \mathbb{N} \rightarrow A$ as funções definidas por

$$f(m) = \begin{cases} m+7 & \text{se } m \text{ é ímpar} \\ 2m+4 & \text{se } m \text{ é par} \end{cases}, \quad h(m) = 2m-1 \quad \text{e} \quad g(m) = 2m+6.$$

- (a) Determine $f(\{3, 4, 5\})$ e $f^{\leftarrow}(\{12, 18\})$. Apresente os cálculos que efetuar.
- (b) Diga, justificando, se f é injetiva e se f é sobrejetiva.
- (c) Verifique que $f \circ h = g$.
- (d) Justifique que a função g é invertível e determine a sua inversa.
- (e) Conclua que a afirmação seguinte nem sempre é verdadeira: Se $f_1 : B \rightarrow C$ e $f_2 : C \rightarrow D$ são funções tais que $f_2 \circ f_1$ é uma função bijetiva, então f_1 e f_2 são funções bijetivas.

resolução:

- (a) Por definição, $f(\{3, 4, 5\}) = \{f(3), f(4), f(5)\}$.

Como 3 e 5 são ímpares,

$$f(3) = 3 + 7 = 10$$

e

$$f(5) = 5 + 7 = 12.$$

Sendo 4 um natural par,

$$f(4) = 2 \times 4 + 4 = 12.$$

Assim, $f(\{3, 4, 5\}) = \{10, 12\}$.

Determinemos, agora, $f^{\leftarrow}(\{12, 18\})$. Por definição,

$$f^{\leftarrow}(\{12, 18\}) = \{m \in \mathbb{N} \mid f(m) = 12 \vee f(m) = 18\}.$$

Ora,

$$\begin{aligned} f(m) = 12 &\Leftrightarrow (m + 7 = 12 \wedge m \text{ é ímpar}) \\ &\vee (2m + 4 = 12 \wedge m \text{ é par}) \\ &\Leftrightarrow (m = 5 \wedge m \text{ é ímpar}) \\ &\vee (m = 4 \wedge m \text{ é par}) \\ &\Leftrightarrow m = 5 \vee m = 4 \end{aligned}$$

e

$$\begin{aligned} f(m) = 18 &\Leftrightarrow (m + 7 = 18 \wedge m \text{ é ímpar}) \\ &\vee (2m + 4 = 18 \wedge m \text{ é par}) \\ &\Leftrightarrow (m = 11 \wedge m \text{ é ímpar}) \\ &\vee (m = 7 \wedge m \text{ é par}) \\ &\Leftrightarrow m = 11. \end{aligned}$$

Assim, $f^{\leftarrow}(\{12, 18\}) = \{4, 5, 11\}$

(b) Da alínea anterior sabemos que $f(4) = f(5) = 12$. Logo, f não é injetiva.

Vejamos se f é sobrejetiva. Para tal, consideremos $x \in A$. Temos que $x \in \mathbb{N}$, $x \geq 8$ e x é par. Consideremos $m = x - 7$. É óbvio que m é um natural ímpar. Além disso, $f(m) = f(x - 7) = (x - 7) + 7 = x$. Provamos, deste modo, que para todos $x \in A$, existe $m \in \mathbb{N}$ tal que $f(m) = x$. Assim, f é sobrejetiva.

(c) O domínio de $f \circ h$ é \mathbb{N} e o conjunto de chegada é A . Também o domínio de g é \mathbb{N} e o conjunto de chegada A . Para concluir que $f \circ h$ é g resta-nos mostrar que $(f \circ h)(m) = g(m)$, para todo $m \in \mathbb{N}$. Dado $m \in \mathbb{N}$,

$$\begin{aligned} (f \circ h)(m) &= f(h(m)) \\ &= f(2m - 1) \\ &= (2m - 1) + 7, \end{aligned}$$

uma vez que $2m - 1$ é ímpar. Assim, para todo $m \in \mathbb{N}$, $(f \circ h)(m) = 2m + 6 = g(m)$. Podemos, pois, concluir que $f \circ h = g$.

(d) Dados $m, n \in \mathbb{N}$, $g(n) = g(m) \implies 2n + 6 = 2m + 6 \implies n = m$. Portanto, g é injetiva. Mais ainda, dado $x \in A$, temos que $m = \frac{x-6}{2}$ é um natural tal que $g(m) = x$. De facto, sendo x par não inferior a 8, $x - 6$ é um natural par e, portanto, $m = \frac{x-6}{2} \in \mathbb{N}$, sendo $g(m) = 2 \times (\frac{x-6}{2}) + 6 = x$. Logo, g é sobrejetiva. Sendo injetiva e sobrejetiva, g é bijetiva e, por isso, invertível. A sua inversa é a função $g^{-1} : A \rightarrow \mathbb{N}$ definida por $g^{-1}(x) = \frac{x-6}{2}$ para todo $x \in A$.

(e) A afirmação é falsa. Com efeito, basta considerar $f_1 = f$ e $f_2 = h$. Por (c) e (d) sabemos que $f_1 \circ f_2$ é bijetiva. No entanto, de (b) sabemos que f_1 não é bijetiva.

2. Considere a função $f : \mathbb{Z} \rightarrow \mathbb{Z}$ definida da seguinte forma

$$f(n) = \begin{cases} 2n + 3 & \text{se } -3 \leq n \leq 1 \\ 3n - 1 & \text{se } n < -3 \text{ ou } n > 1 \end{cases}.$$

- (a) **Determine $f(\{n \in \mathbb{Z} \mid -1 \leq n \leq 2\})$ e $f^{\leftarrow}(\{-5, 3\})$.**
 (b) **Diga, justificando, se f é sobrejetiva e/ou injetiva.**

resolução:

(a) Por definição,

$$f(\{n \in \mathbb{Z} \mid -1 \leq n \leq 2\}) = f(\{-1, 0, 1, 2\}) = \{f(-1), f(0), f(1), f(2)\}.$$

Ora, $f(-1) = 2 \times (-1) + 3 = 1$, $f(0) = 2 \times 0 + 3 = 3$, $f(1) = 2 \times 1 + 3 = 5$ e $f(2) = 3 \times 2 - 1 = 5$. Logo, $f(\{n \in \mathbb{Z} \mid -1 \leq n \leq 2\}) = \{1, 3, 5\}$.

Por definição, $f^{\leftarrow}(\{-5, 3\}) = \{n \in \mathbb{Z} \mid f(n) = -5 \vee f(n) = 3\}$. Temos que

$$\begin{aligned} f(n) = -5 &\Leftrightarrow (2n + 3 = -5 \wedge -3 \leq n \leq 1) \\ &\vee (3n - 1 = -5 \wedge (n < -3 \vee n > 1)) \\ &\Leftrightarrow (n = -4 \wedge -3 \leq n \leq 1) \\ &\vee (3n = -4 \wedge (n < -3 \vee n > 1)), \end{aligned}$$

o que é uma condição impossível em \mathbb{Z} . Assim, não existe nenhum inteiro n cuja imagem, por f , seja -5 . Por outro lado,

$$\begin{aligned} f(n) = 3 &\Leftrightarrow (2n + 3 = 3 \wedge -3 \leq n \leq 1) \\ &\vee (3n - 1 = 3 \wedge (n < -3 \vee n > 1)) \\ &\Leftrightarrow (n = 0 \wedge -3 \leq n \leq 1) \\ &\vee (3n = 4 \wedge (n < -3 \vee n > 1)) \\ &\Leftrightarrow n = 0. \end{aligned}$$

Portanto, existe um só $n \in \mathbb{Z}$ tal que $f(n) = 3$, $n = 0$. Portanto, $f^{\leftarrow}(\{-5, 3\}) = \{0\}$.

(b) Da alínea anterior, sabemos que $f(1) = f(2) = 5$, pelo que f é não injetiva, e que não existe nenhum $n \in \mathbb{Z}$ tal que $f(n) = -5$, donde f é não sobrejetiva.

3. Considere as funções $f : \mathbb{R} \rightarrow \mathbb{R}$ definida por $f(x) = |x| + 2$, para todo o real x , e $g : \mathbb{R} \rightarrow \mathbb{R}$ definida da seguinte forma

$$g(x) = \begin{cases} x^2 & \text{se } x \leq -2 \\ x + 2 & \text{se } x > -2 \end{cases}.$$

- (a) **Determine $f(\{-2, 2\})$ e $f([-2, 4])$.**
 (b) **Determine $f^{\leftarrow}(\{-2, 0, 1, 2\})$.**

(c) Diga se $g \circ f$ é injetiva e se é sobrejetiva.

resolução:

(a) Temos que $f(-2) = |-2| + 2 = 4$ e $f(2) = |2| + 2 = 4$. Assim, $f(\{-2, 2\}) = \{f(-2), f(2)\} = \{4\}$.

Por definição, $f([-2, 4]) = \{f(x) \mid x \in [-2, 4]\}$. f é uma função estritamente decrescente em $]-\infty, 0]$ e estritamente crescente em $[0, +\infty[$. Temos que $f(-2) = 4$, $f(0) = 2$ e $f(4) = 6$. Além disso, todo o elemento y entre 2 e 6 é imagem, por f , de $x = y - 2 \in \mathbb{R}$. Portanto, $f([-2, 4]) = [2, 6]$.

(b) Por definição, $f^{\leftarrow}(\{-2, 0, 1, 2\}) = \{x \in \mathbb{R} \mid f(x) = -2 \vee f(x) = 0 \vee f(x) = 1 \vee f(x) = 2\}$. Temos que

$$\begin{aligned} f(x) = -2 &\Leftrightarrow |x| + 2 = -2 \\ &\Leftrightarrow |x| = -4 \\ &\Leftrightarrow i(x), \end{aligned}$$

$$\begin{aligned} f(x) = 0 &\Leftrightarrow |x| + 2 = 0 \\ &\Leftrightarrow |x| = -2 \\ &\Leftrightarrow i(x), \end{aligned}$$

$$\begin{aligned} f(x) = 1 &\Leftrightarrow |x| + 2 = 1 \\ &\Leftrightarrow |x| = -1 \\ &\Leftrightarrow i(x) \end{aligned}$$

e

$$\begin{aligned} f(x) = 2 &\Leftrightarrow |x| + 2 = 2 \\ &\Leftrightarrow |x| = 0 \\ &\Leftrightarrow x = 0. \end{aligned}$$

Assim, $f^{\leftarrow}(\{-2, 0, 1, 2\}) = \{0\}$

(c) Note-se que $f(x) \geq 2$, para todo $x \in \mathbb{R}$. Portanto, $(g \circ f)(x) = g(f(x)) = f(x) + 2 = |x| + 4$. Dado que $(g \circ f)(-1) = (g \circ f)(1) = 5$, $g \circ f$ não é injetiva. Além disso, $(g \circ f)(x) \geq 4$, para todo $x \in \mathbb{R}$. Assim, não existe nenhum $x \in \mathbb{R}$ tal que $(g \circ f)(x) = 0$ e $g \circ f$ não é sobrejetiva.

Capítulo 5

Relações binárias

A noção de relação entre dois objetos baseia-se na ideia de que esses dois objetos estão associados de alguma forma. Uma relação binária será, então, um conjunto de pares ordenados e os seus elementos serão os pares ordenados (a, b) tais que a está associado a b .

[Definição 5.1] Sejam A e B dois conjuntos. Chamamos **relação binária de A em B** a qualquer subconjunto R do produto cartesiano $A \times B$. Quando $A = B$, dizemos que R é uma **relação binária em A** .

Se $(a, b) \in R$, então dizemos que a **está relacionado com b por R** e escrevemos $a R b$.

Se $(a, b) \notin R$, escrevemos $a \nR b$ e dizemos que a **não está relacionado com b por R** .

[Exemplos]

[1] Sejam $A = \{1, 2\}$ e $B = \{1, 3, 5, 7\}$. São exemplos de relações binárias de A em B os conjuntos

- i. $R = \{(1, 1), (1, 3), (2, 7)\}$;
- ii. $S = \{(2, 3)\}$;
- iii. \emptyset ;
- iv. $A \times B$.

[2] Sejam $A = \{1, 2, 3, 4\}$ e $B = \{1, 3, 4, 8, 9\}$. Então, $R = \{(1, 1), (2, 4), (3, 9)\}$ é uma relação binária de A em B que pode ser definida por

$$a R b \Leftrightarrow b = a^2 \quad (a \in A, b \in B).$$

[3] Sejam $A = \{1, 2, 3\}$ e $B = \{1, 2\}$. Então,

- i. $R = \{(1, 1), (2, 2)\}$ é uma relação binária de A em B ;
- ii. $S = \{(1, 1), (2, 2), (3, 3)\}$ não é uma relação binária de A em B , visto que $S \not\subseteq A \times B$.

[4] Sejam $A = \{1, 2, 3\}$ e $B = \{2, 4, 6, 9, 10\}$.

Se R é a relação binária de A em B definida por $a R b$ se e só se $a|b$ (ou seja, a divide b), então

$$R = \{(1, 2), (1, 4), (1, 6), (1, 9), (1, 10), (2, 2), (2, 4), (2, 6), (2, 10), (3, 6), (3, 9)\}$$

Facilmente verificamos que $2 \not R 9$, pois $2 \nmid 9$. No entanto, $(2, 9) \in A \times B$.

Por outro lado, apesar de $5|10$, temos que $5 \not R 10$, pois $(5, 10) \notin A \times B$.

Dados dois conjuntos A e B , o conjunto de todas as relações binárias de A em B é o conjunto $\mathcal{P}(A \times B)$.

Se os conjuntos A e B forem finitos e tiverem n e m elementos, respetivamente, então $A \times B$ tem $n \times m$ elementos, pelo que $\mathcal{P}(A \times B)$ tem $2^{n \times m}$ elementos. Assim, **existem $2^{n \times m}$ relações binárias de A em B** .

Os conjuntos \emptyset e $A \times B$ são relações binárias de A em B , designadas, respetivamente, por **relação vazia** e **relação universal**.

[Definição 5.2] Seja A um conjunto não vazio. Então,

$$\text{id}_A = \{(a, a) : a \in A\} \text{ e } \omega_A = A^2 = \{(x, y) : x, y \in A\}$$

são relações binárias em A . A id_A chamamos **relação identidade em A** e a ω_A chamamos **relação universal em A** .

[Definição 5.3] Sejam A, B conjuntos e R uma relação binária de A em B . Chamamos **domínio de R** ao conjunto

$$\text{Dom}(R) = \{a \in A \mid \exists b \in B (a, b) \in R\};$$

Chamamos **imagem** ou **contradomínio de R** ao conjunto

$$\text{Im}(R) = \{b \in B \mid \exists a \in A (a, b) \in R\}.$$

[Exemplo]

Consideremos os conjuntos $A = \{2, 4, 5\}$ e $B = \{2, 3, 4, 5\}$ e a relação R de A em B definida por $(a, b) \in R$ se e só se $a < b$. Então,

- i. $R = \{(2, 3), (2, 4), (2, 5), (4, 5)\}$;
- ii. $\text{Dom}(R) = \{2, 4\}$;
- iii. $\text{Im}(R) = \{3, 4, 5\}$.

[Definição 5.4] Duas relações binárias R e S de um conjunto A num conjunto B são **iguais** quando os conjuntos R e S são iguais. Em particular, $\text{Dom}(R) = \text{Dom}(S)$ e $\text{Im}(R) = \text{Im}(S)$.

Note-se, no entanto, que não é necessariamente verdade que $R = S$ sempre que $\text{Dom}(R) = \text{Dom}(S)$ e $\text{Im}(R) = \text{Im}(S)$, como podemos comprovar no exemplo que se segue.

[Exemplo]

Consideremos os conjuntos $A = \{2, 4, 5\}$ e $B = \{2, 3, 4, 5\}$. Seja R a relação de A em B definida por $(a, b) \in R$ se e só se $a < b$ e seja $S = \{(2, 3), (2, 4), (4, 5)\}$. Então,

- i. $\text{Dom}(R) = \{2, 4\} = \text{Dom}(S)$;
- ii. $\text{Im}(R) = \{3, 4, 5\} = \text{Im}(S)$;
- iii. $(2, 5) \in R$ mas $(2, 5) \notin S$, pelo que $R \neq S$.

De seguida, estudamos alguns processos que permitem obter novas relações a partir de relações dadas.

Como uma relação binária é um conjunto, podemos considerar, em particular, os processos estudados anteriormente para obter novos conjuntos a partir de conjuntos dados. Assim, se R e S são relações binárias de A em B , o mesmo acontece com $R \cup S$, $R \cap S$, $R \setminus S$, pois cada um destes conjuntos é ainda um subconjunto de $A \times B$.

[Exemplo]

Consideremos os conjuntos $A = \{2, 4, 5\}$ e $B = \{2, 3, 4, 5\}$ e as relações $R = \{(2, 3), (2, 4), (2, 5), (4, 5)\}$ e $S = \{(2, 3), (2, 4), (4, 5)\}$. Então,

- i. $R \cup S = \{(2, 3), (2, 4), (2, 5), (4, 5)\}$ é uma relação binária de A em B ;
- ii. $R \cap S = \{(2, 3), (2, 4), (4, 5)\}$ é uma relação binária de A em B ;
- iii. $R \setminus S = \{(2, 5)\}$ é uma relação binária de A em B .

Além destes processos para obter novas relações, existem outros que são específicos das relações.

[Definição 5.5] Sejam A, B conjuntos e R uma relação binária de A em B . Chama-se **relação inversa de R** , e representa-se por R^{-1} , a relação de B em A definida por

$$R^{-1} = \{(b, a) \in B \times A \mid (a, b) \in R\}.$$

[Exemplo]

Consideremos, de novo, os conjuntos $A = \{2, 4, 5\}$, $B = \{2, 3, 4, 5\}$ e a relação R de A em B definida por $(a, b) \in R$ se e só se $a < b$. Uma vez que $R = \{(2, 3), (2, 4), (2, 5), (4, 5)\}$ tem-se

$$R^{-1} = \{(3, 2), (4, 2), (5, 2), (5, 4)\}.$$

[Proposição 5.6] Sejam A, B conjuntos e R e S relações binárias de A em B . Então,

- 1 $\mid \text{Dom}(R^{-1}) = \text{Im}(R)$ e $\text{Im}(R^{-1}) = \text{Dom}(R)$.
- 2 $\mid (R^{-1})^{-1} = R$.

3 | Se $R \subseteq S$, então $R^{-1} \subseteq S^{-1}$.

demonstração:

1 | Por definição de domínio de uma relação binária, $\text{Dom}(R^{-1}) = \{b \in B \mid \exists a \in A (b, a) \in R^{-1}\}$. Assim, $\text{Dom}(R^{-1}) = \{b \in B \mid \exists a \in A (a, b) \in R\}$, ou seja, $\text{Dom}(R^{-1}) = \text{Im}(R)$. Por outro lado, por definição de contradomínio de uma relação binária, $\text{Im}(R^{-1}) = \{a \in A \mid \exists b \in B (b, a) \in R^{-1}\}$. Logo, $\text{Im}(R^{-1}) = \{a \in A \mid \exists b \in B (a, b) \in R\}$, isto é, $\text{Im}(R^{-1}) = \text{Dom}(R)$.

2 | Por definição de inversa de uma relação binária,

$$\begin{aligned} (R^{-1})^{-1} &= \{(a, b) \in A \times B \mid (b, a) \in R^{-1}\} \\ &= \{(a, b) \in A \times B \mid (a, b) \in R\} \\ &= R. \end{aligned}$$

3 | Admitamos que $R \subseteq S$. Seja $(b, a) \in R^{-1}$. Então, por definição de inversa de uma relação binária, $(a, b) \in R$. Como $R \subseteq S$, segue-se que $(a, b) \in S$. Logo, $(b, a) \in S^{-1}$. Assim, mostramos que todo o elemento de R^{-1} é elemento de S^{-1} , ou seja, $R^{-1} \subseteq S^{-1}$. ■

Vejamos, de seguida, a definição de relação composta de duas relações binárias.

[Definição 5.7] Sejam A, B, C, D conjuntos, R uma relação binária de A em B e S uma relação binária de C em D . Chama-se **relação composta de S com R** , e representa-se por $S \circ R$, a relação binária de A em D definida por

$$S \circ R = \{(x, y) \in A \times D \mid \exists z \in B \cap C ((x, z) \in R \wedge (z, y) \in S)\}.$$

É de notar que, nas condições da definição anterior, se $B \cap C = \emptyset$, então $S \circ R = \emptyset$.

[Exemplo]

Sejam $A = \{1, 2, 3\}$, $B = \{1, 2, 3, 4, 5\}$, $C = \{0, 2, 3, 4\}$ e $D = \{0, 1, 3, 5\}$. Considere-mos as relações binárias

$$R = \{(1, 2), (1, 3), (2, 2), (2, 4)\} \subseteq A \times B$$

e

$$S = \{(0, 1), (3, 0), (3, 3), (3, 5), (4, 0)\} \subseteq C \times D.$$

Repare-se que, uma vez que $(1, 3) \in R$ e $(3, 0) \in S$, $(1, 0) \in S \circ R$. Temos, também, que $(0, 1) \in S$ e $(1, 2) \in R$, pelo que $(0, 2) \in R \circ S$. Uma análise cuidada, seguindo este tipo de raciocínios, permite-nos concluir que

$$S \circ R = \{(1, 0), (1, 3), (1, 5), (2, 0)\}$$

e

$$R \circ S = \{(0, 2), (0, 3)\}.$$

Do exemplo anterior, podemos concluir que a composição de relações binárias não é necessariamente comutativa: dadas duas relações binárias R e S , nem sempre $R \circ S = S \circ R$.

[Proposição 5.8] Sejam R , S e T relações binárias. Então,

$$1 \mid \text{Dom}(S \circ R) \subseteq \text{Dom}(R) \text{ e } \text{Im}(S \circ R) \subseteq \text{Im}(S).$$

$$2 \mid (T \circ S) \circ R = T \circ (S \circ R).$$

$$3 \mid (S \circ R)^{-1} = R^{-1} \circ S^{-1}.$$

demonstração:

1 | Começemos por mostrar que $\text{Dom}(S \circ R) \subseteq \text{Dom}(R)$. Dado $x \in \text{Dom}(S \circ R)$, existe y tal que $(x, y) \in S \circ R$. Por definição de relação composta, $(x, z) \in R$ e $(z, y) \in S$ para algum z . Em particular, $(x, z) \in R$, pelo que $x \in \text{Dom}(R)$. De forma semelhante prova-se que $\text{Im}(S \circ R) \subseteq \text{Im}(S)$.

2 | Seja $(x, y) \in (T \circ S) \circ R$. Então, $(x, z) \in R$ e $(z, y) \in T \circ S$ para algum z . De $(z, y) \in T \circ S$ segue que $(z, w) \in S$ e $(w, y) \in T$ para algum w . Ora, como $(x, z) \in R$ e $(z, w) \in S$, temos que $(x, w) \in S \circ R$. Assim, $(x, w) \in S \circ R$ e $(w, y) \in T$, pelo que $(x, y) \in T \circ (S \circ R)$. Logo, $(T \circ S) \circ R \subseteq T \circ (S \circ R)$. De modo análogo se prova que $T \circ (S \circ R) \subseteq (T \circ S) \circ R$.

3 | Para todo o objeto (x, y) ,

$$\begin{aligned} (x, y) \in (S \circ R)^{-1} &\Leftrightarrow (y, x) \in S \circ R \\ &\Leftrightarrow \exists_z ((y, z) \in R \wedge (z, x) \in S) \\ &\Leftrightarrow \exists_z ((z, y) \in R^{-1} \wedge (x, z) \in S^{-1}) \\ &\Leftrightarrow \exists_z ((x, z) \in S^{-1} \wedge (z, y) \in R^{-1}) \\ &\Leftrightarrow (x, y) \in R^{-1} \circ S^{-1}. \end{aligned}$$

Logo, $(S \circ R)^{-1} = R^{-1} \circ S^{-1}$. ■

[Observações]

1 | Dados A, B conjuntos, uma relação binária R de A em B **total** (ou seja, $\text{Dom}(R) = A$) e **unívoca** (ou seja, para quaisquer $a \in A, b_1, b_2 \in B$, se $(a, b_1) \in R$ e $(a, b_2) \in R$, então $b_1 = b_2$) determina uma função \mathcal{F}_R de A em B tal que, para todo $a \in A$, $\mathcal{F}_R(a) = b$, onde b é o único elemento de B tal que $(a, b) \in R$.

2 | Reciprocamente, dados A, B conjuntos, uma função $f : A \rightarrow B$ determina uma relação binária de A em B , designada por **gráfico de f** , notada por \mathcal{G}_f e dada por $\mathcal{G}_f = \{(a, f(a)) \mid a \in A\}$, que é total e unívoca.

3 | Estes dois processos são inversos e, para R e f nas condições anteriores, tem-se

$$\mathcal{G}_{\mathcal{F}_R} = R \quad \text{e} \quad \mathcal{F}_{\mathcal{G}_f} = f.$$

4 | Na verdade, no âmbito da Teoria de Conjuntos, o conceito de função não é primitivo: o conceito de função surge do conceito de relação como indicado em 1.

Em seguida, referimos certas propriedades que permitem caraterizar algumas classes especiais de relações binárias.

[Definição 5.9] Sejam A um conjunto e R uma relação binária em A . Dizemos que

- 1 | R é **reflexiva** quando $\forall_{a \in A} (a, a) \in R$;
- 2 | R é **simétrica** quando $\forall_{a, b \in A} ((a, b) \in R \Rightarrow (b, a) \in R)$;
- 3 | R é **antissimétrica** quando $\forall_{a, b \in A} (((a, b) \in R \wedge (b, a) \in R) \Rightarrow a = b)$;
- 4 | R é **transitiva** quando $\forall_{a, b, c \in A} (((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R)$.

Note-se que uma relação binária R em A é antissimétrica se e só se

$$\forall_{a, b \in A} (((a, b) \in R \wedge a \neq b) \Rightarrow (b, a) \notin R).$$

[Exemplos]

Seja A um conjunto.

- [1] A relação id_A é reflexiva, simétrica, transitiva e antissimétrica em A .
- [2] A relação ω_A é reflexiva, simétrica e transitiva em A . Esta relação é antissimétrica se e só se A tem no máximo um elemento.
- [3] A relação \emptyset é simétrica, transitiva e antissimétrica em A . Esta relação é reflexiva se e só se $A = \emptyset$.
- [4] Se $A = \{1, 2, 3, 4\}$ e $R = \{(1, 1), (1, 2), (1, 3), (2, 2), (2, 3), (3, 3), (4, 4)\}$, então:
 - i. uma vez que $(1, 1), (2, 2), (3, 3), (4, 4) \in R$, a relação R é reflexiva;
 - ii. o par $(1, 2)$ é elemento de R , mas $(2, 1) \notin R$, pelo que R não é simétrica;
 - iii. como não existem elementos distintos $a, b \in A$ tais que $(a, b) \in R$ e $(b, a) \in R$, podemos afirmar que a relação R é antissimétrica;
 - iv. R é transitiva, visto que

$$\begin{aligned} ((1, 1) \in R \wedge (1, 1) \in R) &\Rightarrow (1, 1) \in R \\ ((1, 1) \in R \wedge (1, 2) \in R) &\Rightarrow (1, 2) \in R \\ ((1, 1) \in R \wedge (1, 3) \in R) &\Rightarrow (1, 3) \in R \\ ((1, 2) \in R \wedge (2, 2) \in R) &\Rightarrow (1, 2) \in R \\ ((1, 2) \in R \wedge (2, 3) \in R) &\Rightarrow (1, 3) \in R \\ ((1, 3) \in R \wedge (3, 3) \in R) &\Rightarrow (1, 3) \in R \\ ((2, 2) \in R \wedge (2, 2) \in R) &\Rightarrow (2, 2) \in R \\ ((2, 2) \in R \wedge (2, 3) \in R) &\Rightarrow (2, 3) \in R \\ ((2, 3) \in R \wedge (3, 3) \in R) &\Rightarrow (2, 3) \in R \\ ((3, 3) \in R \wedge (3, 3) \in R) &\Rightarrow (3, 3) \in R \\ ((4, 4) \in R \wedge (4, 4) \in R) &\Rightarrow (4, 4) \in R \end{aligned}$$

e o antecedente da implicação $((a, b) \in R \wedge (b, c) \in R) \Rightarrow (a, c) \in R$ é falso para as restantes combinações de valores para a, b e c .

[Proposição 5.10] Sejam A um conjunto e R uma relação binária em A . Então

- 1 | R é reflexiva se e só se $\text{id}_A \subseteq R$;
- 2 | R é simétrica se e só se $R^{-1} = R$;
- 3 | R é transitiva se e só se $R \circ R \subseteq R$;
- 4 | R é antissimétrica se e só se $R \cap R^{-1} \subseteq \text{id}_A$.

demonstração:

1 | R é reflexiva se e só se $(x, x) \in R$, para todo o $x \in A$, ou equivalentemente, todo o elemento de id_A é elemento de R .

2 | Admitamos que R é simétrica. Então, para quaisquer $x, y \in A$, se $(x, y) \in R$ então $(y, x) \in R$. Dado $(x, y) \in R^{-1}$, sabemos, por definição de relação inversa, que $(y, x) \in R$. Como R é simétrica, segue-se que $(x, y) \in R$. Logo, $R^{-1} \subseteq R$. Dado $(x, y) \in R$, sabemos, porque R é simétrica, que $(y, x) \in R$. Assim, pela definição de relação inversa, $(x, y) \in R^{-1}$. Portanto, $R \subseteq R^{-1}$ e, conseqüentemente, $R^{-1} = R$.

Reciprocamente, admitamos que $R^{-1} = R$ e mostremos que R é simétrica. Sejam $x, y \in A$ tais que $(x, y) \in R$. Como $R^{-1} = R$, $(x, y) \in R^{-1}$. Por definição de relação inversa, $(y, x) \in R$. Portanto, para quaisquer $x, y \in A$, se $(x, y) \in R$ então $(y, x) \in R$, ou seja, R é simétrica.

3 | Admitamos que R é transitiva. Dado $(x, y) \in R \circ R$, sabemos que existe, pela definição da relação composta, $z \in R$ tal que $(x, z) \in R$ e $(z, y) \in R$. Sendo R transitiva, como $(x, z) \in R$ e $(z, y) \in R$, segue-se que $(x, y) \in R$. Portanto, todo o elemento de $R \circ R$ é elemento de R , isto é $R \circ R \subseteq R$.

Suponhamos, agora, que $R \circ R \subseteq R$ e mostremos que R é transitiva. Para tal, consideremos $x, y, z \in A$ tais que $(x, y) \in R$ e $(y, z) \in R$. Então, por definição da relação composta $R \circ R$, $(x, z) \in R \circ R$. Como $R \circ R \subseteq R$, todo o elemento de $R \circ R$ é também elemento de R . Portanto, $(x, z) \in R$. Provámos, assim, que para quaisquer $x, y, z \in A$ tais que $(x, y) \in R$ e $(y, z) \in R$, temos $(x, z) \in R$, pelo que R é transitiva.

4 | Admitamos que R é antissimétrica e suponhamos que $R \cap R^{-1} \not\subseteq \text{id}_A$. Então, existem $x, y \in A$ tais que $x \neq y$ e $(x, y) \in R \cap R^{-1}$. Portanto, $(x, y) \in R$ e $(x, y) \in R^{-1}$. Logo, $(x, y) \in R$ e $(y, x) \in R$, o que contraria o facto de R ser antissimétrica. A contradição resultou de supormos que $R \cap R^{-1} \not\subseteq \text{id}_A$. Portanto, $R \cap R^{-1} \subseteq \text{id}_A$.

Reciprocamente, admitamos que $R \cap R^{-1} \subseteq \text{id}_A$ e mostremos que R é antissimétrica. Se $x, y \in A$ são tais que $x \neq y$ e $(x, y) \in R$, então $(y, x) \notin R$. De facto, se $(y, x) \in R$, então $(x, y) \in R^{-1}$. Assim, teríamos $(x, y) \in R \cap R^{-1}$. Mas, como $x \neq y$, $(x, y) \notin \text{id}_A$, o que contrariaria a hipótese $R \cap R^{-1} \subseteq \text{id}_A$. ■

5.1 Relações de equivalência

[Definição 5.11] Seja A um conjunto. Uma relação binária R diz-se uma **relação de equivalência em A** quando R é reflexiva, simétrica e transitiva.

[Exemplos]

[1] Dado um conjunto A não vazio, as relações id_A e ω_A são relações de equivalência em A .

[2] Sejam $A = \{1, 2, 3, 4, 5\}$ e $S = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (1, 2), (2, 1), (3, 4), (4, 3)\}$. Então,

i. S é reflexiva uma vez que

$$id_A = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5)\} \subseteq S;$$

ii. S é simétrica pois

$$S^{-1} = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (1, 2), (4, 3), (3, 4)\} = S;$$

iii. S é transitiva porque

$$S \circ S = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (2, 1), (1, 2), (4, 3), (3, 4)\} \subseteq S.$$

Por i.-iii., S é uma relação de equivalência em A .

[3] Sejam A e B conjuntos e $f : A \rightarrow B$ uma função. A relação binária definida em A por

$$x R_f y \Leftrightarrow f(x) = f(y)$$

é uma relação de equivalência em A . De facto,

i. R_f é reflexiva: $\forall x \in A \ f(x) = f(x)$;

ii. R_f é simétrica: $\forall x, y \in A \ (f(x) = f(y) \Rightarrow f(y) = f(x))$;

iii. R_f é transitiva: $\forall x, y, z \in A \ ((f(x) = f(y) \wedge f(y) = f(z)) \Rightarrow f(x) = f(z))$.

[4] Seja R a relação binária em \mathbb{Z} definida por

$$a R b \Leftrightarrow a - b \text{ é divisível por } 3.$$

Facilmente verificamos que R é uma relação de equivalência. Com efeito,

i. para todo o $a \in \mathbb{Z}$, $a - a = 0$ é divisível por 3, pelo que $a R a$. Portanto, R é reflexiva;

ii. para todos os $a, b \in \mathbb{Z}$, se $a R b$, então $a - b = 3k$, para algum $k \in \mathbb{Z}$, pelo que $b - a = -(a - b) = -(3k) = 3(-k)$, com $-k \in \mathbb{Z}$. Logo, $b R a$ e, assim, R é simétrica;

iii. para todos os $a, b, c \in \mathbb{Z}$, se $a R b$ e $b R c$, então $a - b = 3k$, para algum $k \in \mathbb{Z}$, e $b - c = 3k'$, para algum $k' \in \mathbb{Z}$. Logo, $a - c = (a - b) + (b - c) = 3(k + k')$, com $k + k' \in \mathbb{Z}$, pelo que $a R c$. Logo, R é transitiva.

Notemos que, dado $a \in \mathbb{Z}$,

$$\begin{aligned} 1 R a &\Leftrightarrow 1 - a = 3k, \text{ para algum } k \in \mathbb{Z} \\ &\Leftrightarrow a = 3k + 1, \text{ para algum } k \in \mathbb{Z} \\ &\Leftrightarrow a \text{ tem resto } 1 \text{ na divisão inteira por } 3. \end{aligned}$$

De modo análogo se prova que $2 R a$ se e só se a tem resto 2 na divisão inteira por 3 e $0 R a$ se e só se a tem resto 0 na divisão inteira por 3.

Assim, uma vez que 0, 1, 2 são os únicos restos possíveis na divisão inteira por 3 e R é uma relação de equivalência, os elementos de \mathbb{Z} podem ser agrupados nos seguintes três subconjuntos de \mathbb{Z} :

$$\begin{aligned} X_0 &= \{a \in \mathbb{Z} \mid 0 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k\} \\ X_1 &= \{a \in \mathbb{Z} \mid 1 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k + 1\} \\ X_2 &= \{a \in \mathbb{Z} \mid 2 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k + 2\} \end{aligned}$$

[Definição 5.12] Sejam R uma relação de equivalência num conjunto A e $x \in A$. Chama-se **classe de equivalência de x módulo R** ou, caso não haja ambiguidade, **classe de equivalência de x** , ao conjunto

$$[x]_R = \{y \in A \mid x R y\}.$$

[Exemplos]

[1] Consideremos a relação de equivalência R definida no exemplo anterior. Então,

$$\begin{aligned} [0]_R &= \{a \in \mathbb{Z} \mid 0 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k\}, \\ [1]_R &= \{a \in \mathbb{Z} \mid 1 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k + 1\}, \\ [2]_R &= \{a \in \mathbb{Z} \mid 2 R a\} = \{a \in \mathbb{Z} \mid \exists_{k \in \mathbb{Z}} a = 3k + 2\}. \end{aligned}$$

[2] Seja $A \neq \emptyset$. Consideremos a relação de equivalência id_A . Para $x \in A$, temos que

$$[x]_{id_A} = \{y \in A \mid y id_A x\} = \{y \in A \mid y = x\} = \{x\}.$$

[3] Seja $A \neq \emptyset$. Consideremos a relação de equivalência ω_A . Para $x \in A$, temos que

$$[x]_{\omega_A} = \{y \in A \mid y \omega_A x\} = A,$$

[4] Seja $A = \{1, 2, 3, 4\}$. Consideremos a relação de equivalência $S = \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (4, 4)\}$. Então,

$$[1]_S = \{1, 2\} = [2]_S, \quad [3]_S = \{3\}, \quad [4]_S = \{4\}.$$

[Proposição 5.13] Seja R uma relação de equivalência num conjunto A e sejam $x, y \in A$. Então:

- (a) $x \in [x]_R$;
- (b) $x R y \Leftrightarrow [x]_R = [y]_R$;
- (c) $x \not R y \Leftrightarrow [x]_R \cap [y]_R = \emptyset$.

demonstração:

(a) Sendo R reflexiva, sabemos que $x R x$. Logo, por definição de classe de equivalência, $x \in [x]_R$.

(b) Admitamos que $x R y$. Como R é simétrica, sabemos ainda que $y R x$ e, sendo R transitiva, segue-se que, para todo o elemento z de A ,

$$\begin{aligned} z \in [x]_R &\Leftrightarrow z R x \\ &\Leftrightarrow z R y \\ &\Leftrightarrow z \in [y]_R. \end{aligned}$$

Logo, $[x]_R = [y]_R$.

Reciprocamente, admitamos que $[x]_R = [y]_R$. De (a) sabemos que $x \in [x]_R$. Assim, $x \in [y]_R$, pelo que $x R y$.

(c) Atendendo à reflexividade, à simetria e à transitividade de R , temos que

$$\begin{aligned} [x]_R \cap [y]_R \neq \emptyset &\Leftrightarrow \exists_z z \in [x]_R \cap [y]_R \\ &\Leftrightarrow \exists_z (z \in [x]_R \wedge z \in [y]_R) \\ &\Leftrightarrow \exists_z (z R x \wedge z R y) \\ &\Leftrightarrow \exists_z (x R z \wedge z R y) \\ &\Leftrightarrow x R y. \end{aligned}$$

Logo, $x \not R y \Leftrightarrow [x]_R \cap [y]_R = \emptyset$. ■

Do resultado anterior, podemos afirmar que toda a classe de equivalência é não vazia e que classes de equivalência distintas são disjuntas.

[Definição 5.14] Ao conjunto de todas as classes de equivalência dos elementos de A chamamos **conjunto quociente de A módulo R** e representamo-lo por A/R , ou seja,

$$A/R = \{[x]_R \mid x \in A\}.$$

[Exemplos]

- 1 | Consideremos a relação de equivalência R em \mathbb{Z} do exemplo anterior. Então, $\mathbb{Z}/R = \{[0]_R, [1]_R, [2]_R\}$.
- 2 | Seja $A \neq \emptyset$. Consideremos a relação de equivalência id_A . Temos que $A/id_A = \{\{x\} \mid x \in A\}$.

3 | Seja $A \neq \emptyset$. Consideremos a relação de equivalência ω_A . O respetivo conjunto quociente é $A/\omega_A = \{A\}$.

4 | Consideremos a relação de equivalência S em $A = \{1, 2, 3, 4\}$ do exemplo anterior. Temos que $A/R = \{\{1, 2\}, \{3\}, \{4\}\}$.

[Definição 5.15] Sejam A um conjunto e $\Pi \subseteq \mathcal{P}(A)$. Diz-se que Π é uma **partição do conjunto** A se:

- 1 | para todo $X \in \Pi$, $X \neq \emptyset$;
- 2 | para todos $X, Y \in \Pi$, $(X \neq Y \Rightarrow X \cap Y = \emptyset)$;
- 3 | para todo $a \in A$, existe $X \in \Pi$ tal que $a \in X$.

[Exemplo]

Sejam $A = \{1, 2, 3, 4, 5\}$ e

$$\begin{aligned}\Pi_1 &= \{\{1, 2\}, \{\}, \{3, 4, 5\}\}, & \Pi_2 &= \{\{1, 2\}, \{2, 3\}, \{4, 5\}\}, \\ \Pi_3 &= \{\{1, 2\}, \{4, 5\}\}, & \Pi_4 &= \{\{1, 2\}, \{3\}, \{4, 5\}\}.\end{aligned}$$

Nenhum dos conjuntos Π_1, Π_2, Π_3 é uma partição de A . Com efeito,

$[\Pi_1]$ $\emptyset \in \Pi_1$ e, portanto, o conjunto Π_1 não verifica a condição 1 | da definição anterior.

$[\Pi_2]$ o conjunto Π_2 não satisfaz a condição 2 | : $X = \{1, 2\} \in \Pi_2$, $Y = \{2, 3\} \in \Pi_2$, $X \neq Y$ e $X \cap Y \neq \emptyset$.

$[\Pi_3]$ no caso do conjunto Π_3 falha a condição 3 | : $3 \in A$ e não existe $X \in \Pi_3$ tal que $3 \in X$.

No que diz respeito ao conjunto Π_4 , é simples verificar que qualquer uma das condições 1 |-3 | da definição anterior é satisfeita e, portanto, Π_4 é uma partição de A .

[Exemplos]

1 | O conjunto quociente $\mathbb{Z}/R = \{[0]_R, [1]_R, [2]_R\}$, onde R é a relação de equivalência definida por $a R b \Leftrightarrow a - b$ é divisível por 3, é uma partição de \mathbb{Z} .

2 | Dado $A \neq \emptyset$, temos que $A/\text{id}_A = \{\{x\} \mid x \in A\}$. É claro que A/id_A é uma partição de A .

3 | Dado $A \neq \emptyset$, temos que $A/\omega_A = \{A\}$ e $\{A\}$ é uma partição de A .

4 | Se $A = \{1, 2, 3, 4\}$ e $R = \{(1, 1), (2, 2), (1, 2), (2, 1), (3, 3), (4, 4)\}$, então $A/R = \{\{1, 2\}, \{3\}, \{4\}\}$. Facilmente se verifica que A/R é uma partição de $A = \{1, 2, 3, 4\}$.

Tal como se estabelece no resultado seguinte, a cada relação de equivalência definida num conjunto A está associada uma partição de A .

[Proposição 5.16] Seja R uma relação de equivalência num conjunto A . Então, A/R é uma partição de A .

demonstração:

Note-se que $A/R = \{[x]_R \mid x \in A\}$. Logo, A/R é formado por subconjuntos de A . Além disso, para qualquer $x \in A$, $x \in [x]_R$, pelo que todo o elemento de A/R é um conjunto não vazio e todo o elemento de A pertence a algum elemento de A/R . Mais ainda, se x e y são elementos de A tais que $[x]_R \neq [y]_R$, então $x \not R y$ e $[x]_R \cap [y]_R = \emptyset$. ■

O recíproco do resultado anterior também é válido, ou seja, cada partição de um conjunto define uma relação de equivalência nesse conjunto.

[Proposição 5.17] Sejam A um conjunto, Π uma partição de A e \mathcal{R}_Π a relação binária em A definida por

$$x \mathcal{R}_\Pi y \text{ se e só se existe } X \in \Pi \text{ tal que } x, y \in X.$$

Então, \mathcal{R}_Π é uma relação de equivalência em A .

demonstração:

Dado $x \in A$, sabemos que existe $X \in \Pi$ tal que $x \in X$. Logo, $x \mathcal{R}_\Pi x$. Portanto, \mathcal{R}_Π é reflexiva.

Sejam $x, y \in A$ tais que $x \mathcal{R}_\Pi y$. Então, por definição, existe $X \in \Pi$ tal que $x, y \in X$. É óbvio que X é tal que $y, x \in X$. Portanto, $y \mathcal{R}_\Pi x$. Logo, \mathcal{R}_Π é simétrica.

Sejam $x, y, z \in A$ tais que $x \mathcal{R}_\Pi y$ e $y \mathcal{R}_\Pi z$. Então, por definição, existe $X \in \Pi$ tal que $x, y \in X$ e existe $X' \in \Pi$ tal que $y, z \in X'$. Temos que $y \in X \cap X'$. Portanto, $X \cap X' \neq \emptyset$, donde $X = X'$ e $x, z \in X$. Podemos, então concluir que $x \mathcal{R}_\Pi z$. \mathcal{R}_Π é, pois, transitiva. ■

[Exemplos]

1 | Sejam $A = \{1, 2, 3, 4, 5, 6\}$ e $\Pi = \{\{1, 2, 3\}, \{4, 6\}, \{5\}\}$ uma partição de A . Então,

$$\mathcal{R}_\Pi = \{(1, 1), (2, 2), (3, 3), (1, 2), (2, 1), (1, 3), (3, 1), (2, 3), (3, 2), \\ (4, 4), (6, 6), (4, 6), (6, 4), (5, 5)\}.$$

2 | Sejam $A = \mathbb{Z}$ e $\Pi = \{X_0, X_1, X_2\}$, onde

$$X_0 = \{3k \mid k \in \mathbb{Z}\}, \quad X_1 = \{3k + 1 \mid k \in \mathbb{Z}\}, \quad X_2 = \{3k + 2 \mid k \in \mathbb{Z}\}.$$

Então,

$$x \mathcal{R}_\Pi y \leftrightarrow x - y \text{ é divisível por } 3.$$

[Observações] Sejam A um conjunto, R uma relação de equivalência em A e Π uma partição de A . Então,

1 | A/R é uma partição de A e

$$\mathcal{R}_{A/R} = R.$$

2 | \mathcal{R}_Π é uma relação de equivalência em A e

$$A/(\mathcal{R}_\Pi) = \Pi.$$

5.2 Relações de de ordem parcial

[Definição 5.18] Seja A um conjunto. Uma relação binária R diz-se uma **relação de ordem parcial em A** quando R é reflexiva, antissimétrica e transitiva. Neste caso, ao par (A, R) dá-se a designação de **conjunto parcialmente ordenado (c.p.o.)**.

[Exemplos]

São exemplos de c.p.o.'s os seguintes pares:

1 | (A, id_A) , onde A é um conjunto e $\text{id}_A = \{(a, a) : a \in A\}$.

2 | (\mathbb{N}, \leq) , onde \leq é a relação “menor ou igual” usual em \mathbb{N} (para todo $x \in \mathbb{N}$, $x \leq x$, logo \leq é reflexiva; para todos $x, y \in \mathbb{N}$, se $x \leq y$ e $y \leq x$, então $x = y$ e, portanto, \leq é antissimétrica; para todos $x, y, z \in \mathbb{N}$, se $x \leq y$ e $y \leq z$, então $x \leq z$, pelo que \leq é transitiva).

3 | $(\mathbb{N}, |)$, onde $|$ é a relação “divide” em \mathbb{N} .

4 | $(\mathcal{P}(A), \subseteq)$, onde A é um conjunto qualquer e \subseteq é a relação de inclusão usual.

Se não houver ambiguidade, representamos uma ordem parcial num conjunto A por \leq e o respetivo c.p.o. por (A, \leq) .

Dado um c.p.o. (A, \leq) e dados $a, b \in A$, escrevemos

$a \leq b$ e lemos “ a é menor ou igual a b ” ou “ a precede b ” para representar $(a, b) \in \leq$;

$a \not\leq b$ e lemos “ a não é menor ou igual a b ” se $(a, b) \notin \leq$;

$a < b$ e lemos “ a é menor do que b ” ou “ a precede propriamente b ” se $a \leq b$ e $a \neq b$;

$a << b$ e lemos “ b é sucessor de a ” ou “ a é sucedido por b ” ou “ b cobre a ” ou “ a é coberto por b ” se $a < b$ e $\neg(\exists c \in A (a < c \wedge c < b))$.

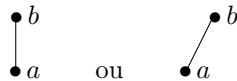
[Definição 5.19] Dado um c.p.o. (A, \leq) e dados $a, b \in A$, dizemos que a, b são **comparáveis** quando $a \leq b$ ou $b \leq a$. Por outro lado, quando $a \not\leq b$ e $b \not\leq a$, dizemos que a e b são **incomparáveis** e escrevemos $a \parallel b$.

Um c.p.o. (A, \leq) , em que A é um conjunto finito não vazio, pode ser representado por meio de um **diagrama de Hasse**, como se descreve em seguida.

1 | cada elemento $a \in A$ é representado por um ponto do plano:

$\bullet a$

2 | se a e b são dois elementos de A tais que $a \leq b$, representa-se b acima de a ; além disso, se $a < b$ unem-se estes dois pontos por um segmento de reta.

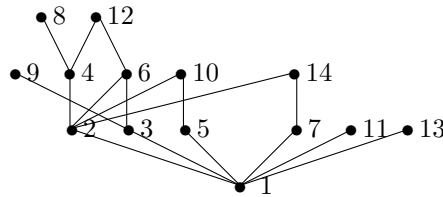


[Exemplos]

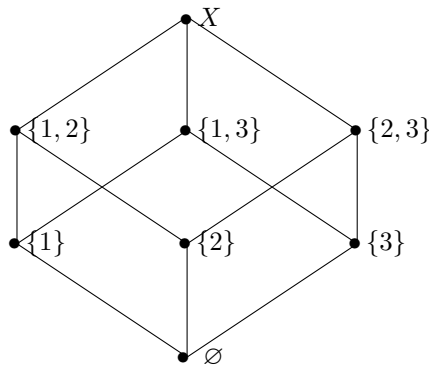
1 | Sejam $A = \{1, 2, 3, 4, 5, 6, 7, 8, 9, 10, 11, 12, 13, 14\}$ e | a ordem parcial definida por

$$x|y \Leftrightarrow \exists_{k \in \mathbb{N}} y = kx.$$

O c.p.o. $(A, |)$ pode ser representado pelo seguinte diagrama de Hasse:



2 | Seja $X = \{1, 2, 3\}$. O c.p.o. $(\mathcal{P}(X), \subseteq)$ pode ser representado pelo diagrama de Hasse que se segue.



Dados um c.p.o. (A, \leq) e X um subconjunto de A , podem existir elementos com propriedades especiais relativamente a X .

[Definição 5.20] Sejam (A, \leq) um c.p.o., X um subconjunto de A e $m \in A$. Dizemos que m é:

1 | um **elemento maximal de X** quando $m \in X$ e $\neg(\exists_{x \in X} m < x)$;

2 | um **elemento minimal de X** quando $m \in X$ e $\neg(\exists_{x \in X} x < m)$;

3 | **majorante de X** quando $\forall_{x \in X} x \leq m$;

- 4 | **minorante de X** quando $\forall_{x \in X} m \leq x$;
- 5 | **supremo de X** quando m é majorante de X e $m \leq m'$, para qualquer m' majorante de X ;
- 6 | **ínfimo de X** quando m é minorante de X e $m' \leq m$, para qualquer m' minorante de X ;
- 7 | **máximo de X** quando m é majorante de X e $m \in X$;
- 8 | **mínimo de X** quando m é minorante de X e $m \in X$.

O conjunto dos majorantes de X e o conjunto dos minorantes de X são representados por $\text{Maj}(X)$ e $\text{Min}(X)$, respetivamente.

Caso exista, o supremo (resp.: ínfimo, máximo, mínimo) de um subconjunto X de A é único e representa-se por $\sup(X)$ (resp.: $\inf(X)$, $\max(X)$, $\min(X)$).

Note-se que, em particular, A tem um máximo se existir $m \in A$ tal que $x \leq m$, para todo $x \in A$; A tem elemento mínimo se existir $m \in A$ tal que $m \leq x$, para todo $x \in A$.

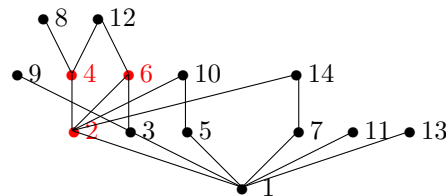
[Exemplo]

Consideremos, de novo, o c.p.o. $(A, |)$ do exemplo anterior

Os elementos maximais de A são o 8, o 9, o 10, o 11, o 12, o 13 e o 14; 1 é o único elemento minimal de A . Além disso,

$$\begin{aligned} \text{Min}(A) &= \{1\}, & \text{Maj}(A) &= \emptyset, & \inf(A) &= 1, \\ \min(A) &= 1, & \sup(A) &\text{ não existe, } & \max(A) &\text{ não existe.} \end{aligned}$$

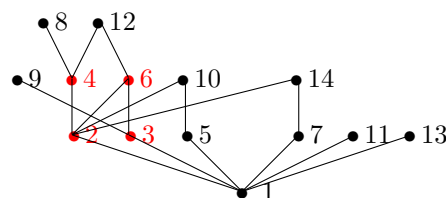
Consideremos o subconjunto $X = \{2, 4, 6\}$ de A .



Os elementos maximais de X são o 4 e o 6; 2 é o único elemento minimal de X . Além disso,

$$\begin{aligned} \text{Min}(X) &= \{1, 2\}, & \text{Maj}(X) &= \{12\}, & \inf(X) &= 2, \\ \min(X) &= 2, & \sup(X) &= 12, & \max(X) &\text{ não existe.} \end{aligned}$$

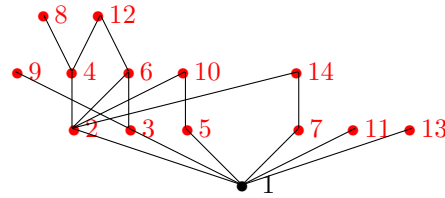
Consideremos, agora, o subconjunto $Y = \{2, 3, 4, 6\}$ de A .



Os elementos maximais de Y são o 4 e o 6; 2 e 3 são os elementos minimais de Y . Além disso,

$$\begin{aligned} \text{Min}(Y) &= \{1\}, & \text{Maj}(Y) &= \{12\}, & \inf(Y) &= 1, \\ \min(Y) &\text{ não existe}, & \sup(Y) &= 12, & \max(Y) &\text{ não existe}. \end{aligned}$$

Consideremos, agora, o subconjunto $Z = A \setminus \{1\}$ de A



Os elementos maximais de Z são: 8, 9, 10, 11, 12, 13 e 14; os elementos minimais de Z são: 2, 3, 5, 7, 11 e 13. Além disso,

$$\begin{aligned} \text{Min}(Z) &= \{1\}, & \text{Maj}(Z) &= \emptyset, & \inf(Z) &= 1, \\ \min(Z) &\text{ não existe}, & \sup(Z) &\text{ não existe}, & \max(Z) &\text{ não existe}. \end{aligned}$$

[Proposição 5.21] Num c.p.o. (A, \leq) , são equivalentes as seguintes afirmações, para quaisquer $a, b \in A$:

- 1 | $a \leq b$;
- 2 | $\sup\{a, b\} = b$;
- 3 | $\inf\{a, b\} = a$.

demonstração:

1 \Rightarrow 2: Se $a \leq b$, como também $b \leq b$, é imediato que $\sup\{a, b\} = b$.

2 \Rightarrow 3: Se $\sup\{a, b\} = b$, então $a \leq b$. Dado que também $a \leq a$, segue-se que $\inf\{a, b\} = a$.

3 \Rightarrow 1: Se $\inf\{a, b\} = b$, então $a \leq b$. ■

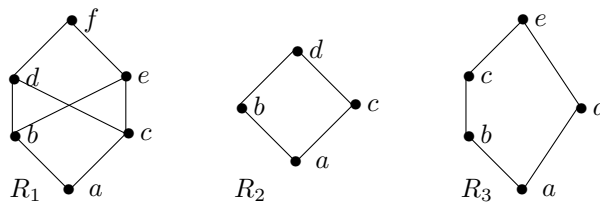
Em seguida, consideramos algumas classes especiais de c.p.o.'s.

[Definição 5.22] Um c.p.o. (A, \leq) diz-se um **reticulado** quando, para quaisquer $x, y \in A$, existem o supremo e o ínfimo do conjunto $\{x, y\}$.

Note-se que, num c.p.o. arbitrário (A, \leq) , dados x, y comparáveis, existem o supremo e o ínfimo do conjunto $\{x, y\}$ (ver proposição anterior). No entanto, se x e y são elementos incomparáveis, já não é garantida a existência de $\sup\{x, y\}$ ou de $\inf\{x, y\}$. Assim, para verificar se um c.p.o. é um reticulado, basta averiguar a existência de $\sup\{x, y\}$ e $\inf\{x, y\}$ para todos os elementos x, y incomparáveis.

[Exemplo]

Consideremos os c.p.o.'s representados pelos seguintes diagramas:



Os c.p.o.'s R_2 e R_3 são reticulados, mas o c.p.o. R_1 não é um reticulado:

R_1 | Os únicos pares de elementos incomparáveis são: b, c e d, e . Temos que $\text{Maj}(\{b, c\}) = \{d, e, f\}$. Sendo d e e incomparáveis, não existe supremo de $\{b, c\}$.

R_2 | O único par de elementos incomparáveis é b, c . Temos que $\text{Maj}(\{b, c\}) = \{d\}$ e $\text{Min}(\{b, c\}) = \{a\}$. Logo, $\sup\{b, c\} = d$ e $\inf\{b, c\} = a$.

R_3 | Os únicos pares de elementos incomparáveis são: b, d e c, d . Temos que $\text{Maj}(\{b, d\}) = \{e\}$, $\text{Min}(\{b, d\}) = \{a\}$, $\text{Maj}(\{c, d\}) = \{e\}$ e $\text{Min}(\{c, d\}) = \{a\}$. Assim, $\sup\{b, d\} = e$, $\inf\{b, d\} = a$, $\sup\{c, d\} = e$ e $\inf\{c, d\} = a$.

[Definição 5.23] Uma ordem parcial \leq num conjunto A diz-se uma **ordem total** ou **ordem linear** quando quaisquer elementos a e b de A são comparáveis. Neste caso, (A, \leq) diz-se uma **cadeia** ou um **conjunto totalmente ordenado**. Um subconjunto X de A diz-se uma **cadeia em** (A, \leq) ou um **subconjunto totalmente ordenado de** (A, \leq) quando, para quaisquer $x, y \in X$, x e y são comparáveis.

[Exemplos]

1 | $\{3, 6, 12\}$ e $\{2, 4\}$ são cadeias em $(\{1, 2, 3, 4, 6, 10, 12\}, |)$, mas este c.p.o. não é uma cadeia, pois 4 e 10 são incomparáveis.

2 | (\mathbb{N}, \leq) , (\mathbb{Z}, \leq) , (\mathbb{R}, \leq) são cadeias.

[Observação] Toda a cadeia é um reticulado, mas o recíproco não se verifica. De facto, numa cadeia quaisquer dois elementos x, y são comparáveis. Logo, existem $\sup\{x, y\}$ e $\inf\{x, y\}$, pelo que qualquer cadeia é um reticulado. O reticulado R_2 do exemplo anterior não é uma cadeia, uma vez que os elementos b e c são incomparáveis.

5.3 Exercícios resolvidos

1. Sejam $A = \{1, 2, 3\}$ e $B = \{x, y, z\}$. Considere as relações binárias R , de A em B , e S , de B em A :

$$R = \{(1, x), (1, z), (2, z)\}$$

$$S = \{(x, 1), (x, 3), (y, 2), (z, 2)\}.$$

- Indique o domínio e a imagem de R .
- Determine R^{-1} , S^{-1} , $R \cup S^{-1}$, $R^{-1} \cap S$, $S \circ R$ e $R \circ S$.
- Dê um exemplo de uma relação binária T , de B em A , tal que $T \circ R = \{(1, 1), (1, 2)\}$.
- Indique quantas relações binárias de A em B existem.
- Indique todas as relações binárias de A em B cujo domínio é $\{1, 2\}$ e cuja imagem é $\{x, y\}$.

resolução:

(a) Temos que $\text{Dom}(R) = \{1, 2\}$ e $\text{Im}(R) = \{x, z\}$.

(b)

$$R^{-1} = \{(x, 1), (z, 1), (z, 2)\}$$

$$S^{-1} = \{(1, x), (3, x), (2, y), (2, z)\}$$

$$\begin{aligned} R \cup S^{-1} &= \{(1, x), (1, z), (2, z)\} \cup \{(1, x), (3, x), (2, y), (2, z)\} \\ &= \{(1, x), (1, z), (2, z), (3, x), (2, y)\} \end{aligned}$$

$$\begin{aligned} R^{-1} \cap S &= \{(x, 1), (z, 1), (z, 2)\} \cap \{(x, 1), (x, 3), (y, 2), (z, 2)\} \\ &= \{(x, 1), (z, 2)\} \end{aligned}$$

$$S \circ R = \{(1, 1), (1, 3), (1, 2), (2, 2)\}$$

$$R \circ S = \{(x, x), (x, z), (y, z), (z, z)\}$$

(c) Para que $(1, 1)$ seja elemento de $T \circ R$, como os únicos pares de R cuja primeira componente é 1 são $(1, x)$ e $(1, z)$, pelo menos um dos elementos $(x, 1)$ ou $(z, 1)$ tem de pertencer a T . Como $(2, z) \in R$, se $(z, 1)$ pertencesse a T teríamos $(2, 1) \in T \circ R$, o que não acontece. Logo, $(z, 1) \notin T$, pelo que $(x, 1) \in T$. De modo semelhante, para que $(1, 2)$ seja elemento de $T \circ R$, pelo menos um dos elementos $(x, 2)$ ou $(z, 2)$ tem de pertencer a T . Como $(2, z) \in R$, se $(z, 2)$ pertencesse a T teríamos $(2, 2) \in T \circ R$. Portanto, $(z, 2) \notin T$, donde $(x, 2) \in T$. Note-se que, se $T = \{(x, 1), (x, 2)\}$, então $T \circ R = \{(1, 1), (1, 2)\}$. No entanto, esta não é a única resposta possível: por exemplo, $T = \{(x, 1), (x, 2), (y, 1)\}$ também satisfaz $T \circ R = \{(1, 1), (1, 2)\}$.

(d) As relações binárias de A em B são os subconjuntos de $A \times B$. Como A e B têm 3 elementos cada, $A \times B$ tem 9 elementos. Logo, existem 2^9 subconjuntos de $A \times B$, ou seja, existem 2^9 relações binárias de A em B .

(e) Para que o domínio de uma relação binária R , de A em B , seja $\{1, 2\}$, tem de existir pelo menos um elemento b_1 de B tal que $(1, b_1) \in R$ e tem de existir pelo menos um elemento b_2 de B tal que $(2, b_2) \in R$. Além disso, não pode haver, em R , nenhum par da forma $(3, b)$, com $b \in B$.

Analogamente, para que a imagem de uma relação binária R , de A em B , seja $\{x, y\}$, tem de existir pelo menos um elemento a_1 de A tal que $(a_1, x) \in R$ e tem de existir pelo menos um elemento a_2 de A tal que $(a_2, y) \in R$. Além disso, não pode haver, em R , nenhum par da forma (a, z) , com $a \in A$.

Conjugando estas condições, podemos concluir que os elementos de uma tal relação binária podem ser $(1, x)$, $(1, y)$, $(2, x)$ ou $(2, y)$, tendo que existir na relação pelo menos um destes pares cuja primeira componente é 1, pelo menos um cuja primeira componente é 2, pelo menos um cuja segunda componente é x e pelo menos um cuja segunda componente é y .

Assim, as relações binária de A em B nas condições do enunciado são

$$\begin{aligned} R_1 &= \{(1, x), (2, y)\} \\ R_2 &= \{(1, y), (2, x)\} \\ R_3 &= \{(1, x), (1, y), (2, y)\} \\ R_4 &= \{(1, x), (2, x), (2, y)\} \\ R_5 &= \{(1, x), (1, y), (2, x)\} \\ R_6 &= \{(1, y), (2, x), (2, y)\} \\ R_7 &= \{(1, x), (1, y), (2, x), (2, y)\}. \end{aligned}$$

2. Considere o conjunto $A = \{1, 2, 3\}$ e a relação binária

$$R = \{(1, 1), (1, 2), (2, 1), (2, 2), (2, 3), (3, 2), (3, 3)\}$$

em A . Indique se R é reflexiva, simétrica, antissimétrica ou transitiva.

resolução:

Como $(1, 1), (2, 2), (3, 3) \in R$, temos que, para todo $x \in A$, $(x, x) \in R$. Logo, R é reflexiva.

Dado que $R^{-1} = \{(1, 1), (2, 1), (1, 2), (2, 2), (3, 2), (2, 3), (3, 3)\} = R$, R é simétrica (note-se que para quaisquer $x, y \in A$, se $(x, y) \in R$ então $(y, x) \in R$).

Dado que $(1, 2), (2, 1) \in R$, R não é antissimétrica (note-se que $R \cap R^{-1} = R \not\subseteq \text{id}_A$).

Temos que $(1, 2) \in R$ e $(2, 3) \in R$. No entanto, $(1, 3) \notin R$. Logo, R não é transitiva (note-se que $R \circ R = \omega_A \not\subseteq R$).

3. Considere o conjunto $A = \{1, 2, 3, 4\}$. Determine a menor relação binária R em A que seja simétrica, transitiva e que contenha os pares $(1, 2)$ e $(2, 4)$.

resolução:

Como $(1, 2) \in R$ e $(2, 4) \in R$, para que R seja transitiva, temos de ter $(1, 4) \in R$. Para que R seja simétrica, como $(1, 2), (2, 4), (1, 4) \in R$, temos de ter $(2, 1), (4, 2), (4, 1) \in R$. Assim, $(1, 2), (2, 1) \in R$, donde, para que R seja transitiva, $(1, 1), (2, 2)$ têm de ser elementos de R . Temos também que $(4, 1), (1, 4) \in R$, pelo que $(4, 4)$ tem de pertencer a R . Note-se que $R = \{(1, 1), (1, 2), (1, 4), (2, 1), (2, 2), (2, 4), (4, 1), (4, 2), (4, 4)\}$ é simétrica, transitiva e contém os pares $(1, 2)$ e $(2, 4)$ e é a menor relação binária em A que satisfaz estas condições.

4. Seja $A = \{1, 2, 5, 7, 8, 9, 15, 27\}$ e considere a relação de equivalência R em A definida por $x R y$ se e só se x e y têm o mesmo número de divisores naturais. Determine $[9]_R$ e determine o conjunto quociente A/R .

resolução:

O único divisor natural de 1 é o 1. Os divisores naturais de 2 são o 1 e o 2. Os divisores naturais de 5 são o 1 e o 5. Os divisores naturais de 8 são o 1, o 2, o 4 e o 8. Os divisores naturais de 9 são o 1, o 3 e o 9. Os divisores naturais de 15 são o 1, o 3, o 5 e o 15. Os divisores naturais de 27 são o 1, o 3, o 9 e o 27. Assim, o 1 tem um divisor natural, o 2 e o 5 têm dois divisores naturais, o 9 tem três divisores naturais e o 8, o 15 e o 27 têm quatro divisores naturais.

Assim,

$$\begin{aligned} [9]_R &= \{x \in A \mid x R 9\} \\ &= \{x \in A \mid x \text{ e } 9 \text{ têm o mesmo número de divisores naturais}\} \\ &= \{x \in A \mid x \text{ tem três divisores naturais}\} \\ &= \{9\}, \end{aligned}$$

uma vez que 9 é o único elemento de A que tem três divisores naturais.

Note-se que 2 e 5 têm o mesmo número de divisores naturais, pelo que $[2]_R = [5]_R$. Porque 8, 15 e 27 têm o mesmo número de divisores naturais, $[8]_R = [15]_R = [27]_R$. Temos que

$$\begin{aligned}
A/R &= \{[x]_R \mid x \in A\} = \{[1]_R, [2]_R, [8]_R, [9]_R\} \\
&= \{\{1\}, \{2, 5\}, \{8, 15, 27\}, \{9\}\}.
\end{aligned}$$

5. Seja $A = \{000, 001, 010, 011, 100, 101, 110, 111\}$, ou seja, A é o conjunto das palavras de comprimento 3 sobre o alfabeto $\{0, 1\}$. Considere a relação binária R em A definida por $x R y$ se e só se x tem o mesmo número de 1's que y .

(a) Mostre que R é uma relação de equivalência em A .

(b) Determine $[101]_R$.

(c) Determine A/R .

resolução:

(a) Dado $x \in A$, é óbvio que x tem o mesmo número de 1's que x . Logo, $x R x$, para todo $x \in A$ e R é reflexiva.

Admitamos, agora, que $x, y \in A$ são tais que $x R y$. Então, x tem o mesmo número de 1's que y , pelo que é claro que y tem o mesmo número de 1's que x , isto é, $y R x$. Portanto, R é simétrica.

Dados $x, y, z \in A$ tais que $x R y$ e $y R z$, temos que x tem o mesmo número de 1's que y e y tem o mesmo número de 1's que z . Logo, x, y e z têm o mesmo número de 1's. Em particular, x tem o mesmo número de 1's que z , donde se segue que $x R z$. Assim, R é transitiva.

Sendo reflexiva, simétrica e transitiva, R é uma relação de equivalência.

(b) Por definição,

$$\begin{aligned}
[101]_R &= \{x \in A \mid x R 101\} \\
&= \{x \in A \mid x \text{ tem o mesmo número de 1's que } 101\} \\
&= \{x \in A \mid x \text{ tem dois 1's}\} \\
&= \{011, 101, 110\}.
\end{aligned}$$

(c) Note-se que 000 tem zero 1's, 001, 010 e 100 têm um 1, 011, 101 e 110 têm dois 1's e 111 tem três 1's. Assim, $[001]_R = [010]_R = [100]_R$ e $[011]_R = [101]_R = [110]_R$. Temos que

$$\begin{aligned}
A/R &= \{[x]_R \mid x \in A\} = \{[000]_R, [001]_R, [011]_R, [111]_R\} \\
&= \{\{000\}, \{001, 010, 100\}, \{011, 101, 110\}, \{111\}\}.
\end{aligned}$$

6. Sejam $A = \{1, 2, 3, 4, 5, 6\}$ e S a relação de equivalência em A tal que $A/S = \{\{1, 3\}, \{2, 4, 6\}, \{5\}\}$. Determine S .

resolução:

Temos que $[1]_S = [3]_S = \{1, 3\}$, $[2]_S = [4]_S = [6]_S = \{2, 4, 6\}$ e $[5]_S = \{5\}$. Logo,

$$R = \{(1, 1), (2, 2), (3, 3), (4, 4), (5, 5), (6, 6), (1, 3), (3, 1), (2, 4), (4, 2), (2, 6), (6, 2), (4, 6), (6, 4)\}.$$

7. Sejam A um conjunto e R a relação de equivalência em $\mathcal{P}(A)$ definida por

$$X R Y \text{ sse } X \cup \{3\} = Y \cup \{3\},$$

para quaisquer $X, Y \in \mathcal{P}(A)$.

- (a) Mostre que a relação binária R é, efetivamente, transitiva.
- (b) Considere $A = \{1, 2, 3\}$. Determine $[\{2, 3\}]_R$ e $\mathcal{P}(A)/R$.
- (c) Dê um exemplo, ou justifique que não existe um exemplo, de um conjunto não vazio A tal que R é a relação universal em $\mathcal{P}(A)$.

resolução:

(a) Dados $X, Y, Z \in \mathcal{P}(A)$ tais que $X R Y$ e $Y R Z$, temos que $X \cup \{3\} = Y \cup \{3\}$ e $Y \cup \{3\} = Z \cup \{3\}$. Consequentemente, $X \cup \{3\} = Z \cup \{3\}$. Logo, para quaisquer $X, Y, Z \in \mathcal{P}(A)$, se $X R Y$ e $Y R Z$, então $X R Z$, ou seja, R é transitiva.

(b) Por definição,

$$\begin{aligned} [\{2, 3\}]_R &= \{X \in \mathcal{P}(A) \mid X R \{2, 3\}\} \\ &= \{X \in \mathcal{P}(A) \mid X \cup \{3\} = \{2, 3\} \cup \{3\}\} \\ &= \{X \in \mathcal{P}(A) \mid X \cup \{3\} = \{2, 3\}\} \\ &= \{\{2\}, \{2, 3\}\} \end{aligned}$$

[obs: note-se que $\mathcal{P}(A) = \{\emptyset, \{1\}, \{2\}, \{3\}, \{1, 2\}, \{1, 3\}, \{2, 3\}, \{1, 2, 3\}\}$]

Temos, que $\emptyset \cup \{3\} = \{3\} = \{3\} \cup \{3\}$. Logo, $[\emptyset]_R = [\{3\}]_R$. Como $\{1\} \cup \{3\} = \{1, 3\} = \{1, 3\} \cup \{3\}$, $[\{1\}]_R = [\{1, 3\}]_R$. Atendendo a que $\{1, 2\} \cup \{3\} = \{1, 2, 3\} = \{1, 2, 3\} \cup \{3\}$, $[\{1, 2\}]_R = [\{1, 2, 3\}]_R$. Assim,

$$\begin{aligned} \mathcal{P}(A)/R &= \{[\emptyset]_R, [\{1\}]_R, [\{2\}]_R, [\{1, 2\}]_R\} \\ &= \{\{\emptyset, \{3\}\}, \{\{1\}, \{1, 3\}\}, \{\{2\}, \{2, 3\}\}, \{\{1, 2\}, \{1, 2, 3\}\}\}. \end{aligned}$$

(c) Seja $A = \{3\}$. Temos que $\mathcal{P}(A) = \{\emptyset, \{3\}\}$. Como $\emptyset \cup \{3\} = \{3\} = \{3\} \cup \{3\}$, $\emptyset R \{3\}$ e $\{3\} R \emptyset$. Além disso, $\emptyset R \emptyset$ e $\{3\} R \{3\}$. Portanto, R é a relação universal em $\mathcal{P}(A)$.

8. Sejam $A = \{1, 2, 3, 4, 5, 6, 7, 8\}$ e R a menor relação de equivalência em A que contém $(1, 4)$, $(3, 4)$ e $(2, 8)$. Determine R .

resolução:

Sendo R reflexiva, $\text{id}_A \subseteq R$. Como $(1, 4), (3, 4), (2, 8) \in R$, sendo R simétrica, $(4, 1), (4, 3), (8, 2) \in R$. Da transitividade de R e porque $(1, 4) \in R \wedge (4, 3) \in R$, segue-se que $(1, 3) \in R$. Sendo R simétrica, temos $(3, 1) \in R$. Assim,

$$\begin{aligned} R = \{ & (1, 1), (1, 3), (1, 4), (2, 2), (2, 8), (3, 1), (3, 3), (3, 4), (4, 1), (4, 3), \\ & (4, 4), (5, 5), (6, 6), (7, 7), (8, 2), (8, 8) \}. \end{aligned}$$

9. Diga, justificando, se são verdadeiras ou falsas as afirmações seguintes:

- (a) Existe uma relação de equivalência ρ em \mathbb{Z} tal que $\mathbb{Z}/\rho = \{\mathbb{Z} \setminus \{1, 2, 3\}, \{2\}, \{1, 3\}\}$.

(b) Existe uma relação de equivalência ρ em \mathbb{Z} tal que $[1]_\rho = \mathbb{Z} \setminus \{2, 3\}$ e $[2]_\rho = \{1, 2, 6\}$.

resolução:

(a) Facilmente se verifica que $\{\mathbb{Z} \setminus \{1, 2, 3\}, \{2\}, \{1, 3\}\}$ é uma partição de \mathbb{Z} . Logo, designando por Π essa partição, sabemos que \mathcal{R}_Π , definida por

$$x \mathcal{R}_\Pi y \text{ se e só se } \text{ existe } X \in \Pi \text{ tal que } x, y \in X,$$

é uma relação de equivalência em \mathbb{Z} . Note-se que todos os elementos de $\mathbb{Z} \setminus \{1, 2, 3\}$ estão relacionados entre si por \mathcal{R}_Π e que nenhum deles está relacionado por \mathcal{R}_Π com 1, 2 ou 3, que 2 apenas está relacionado por \mathcal{R}_Π consigo mesmo e que $(1, 1), (1, 3), (3, 1), (3, 3) \in \mathcal{R}_\Pi$. A afirmação é, portanto, verdadeira.

(b) A afirmação é falsa. Se existisse uma tal relação de equivalência ρ , de $[1]_\rho = \mathbb{Z} \setminus \{2, 3\}$ sabemos que $(1, 2), (2, 1) \notin \rho$ e de $[2]_\rho = \{1, 2, 6\}$ segue-se que $(1, 2), (2, 1) \in \rho$, o que é uma contradição.

10. Considere, no conjunto $A = \{1, 2, 3, 4, 5\}$ as relações de equivalência R e S definidas pelas partições $\Pi_1 = \{\{1, 2\}, \{3\}, \{4, 5\}\}$ e $\Pi_2 = \{\{1, 2, 4\}, \{3, 5\}\}$ de A , respetivamente. Determine o conjunto quociente de A módulo $R \cap S$.

resolução:

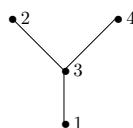
Por definição, dados $x, y \in A$, $x R \cap S y$ se e só se $x R y$ e $x S y$. Logo, $y \in [x]_{R \cap S}$ se e somente se $y \in [x]_R$ e $y \in [x]_S$. Temos que $[1]_R = [2]_R = \{1, 2\}$, $[4]_R = [5]_R = \{4, 5\}$ e $[3]_R = \{3\}$. Além disso, $[1]_S = [2]_S = [4]_S = \{1, 2, 4\}$ e $[3]_S = [5]_S = \{3, 5\}$. Apenas o 1 e o 2 estão na mesma classe de equivalência tanto em R como em S . Assim, $[1]_{R \cap S} = [2]_{R \cap S} = \{1, 2\}$ e as classes de equivalência dos outros elementos de A são apenas formadas pelo próprio elemento. Logo,

$$A/(R \cap S) = \{\{1, 2\}, \{3\}, \{4\}, \{5\}\}.$$

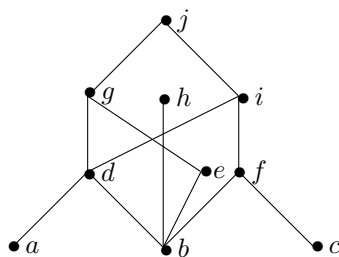
11. Considere o conjunto $A = \{1, 2, 3, 4\}$. Seja R a menor relação de ordem parcial em A tal que $(1, 3), (3, 2), (3, 4) \in R$. Determine R e apresente o diagrama de Hasse associado a esta relação de ordem parcial.

resolução:

Por definição, R terá de ser reflexiva, antissimétrica e transitiva. Sendo R reflexiva, $(1, 1), (2, 2), (3, 3), (4, 4) \in R$. Para quaisquer $a, b \in A$ distintos, se $(a, b) \in R$ então $(b, a) \notin R$, uma vez que R é antissimétrica. Como $(1, 3) \in R$ e $(3, 2) \in R$, sendo R transitiva, $(1, 2) \in R$. Dado que $(1, 3) \in R$ e $(3, 4) \in R$, como R é transitiva, $(1, 4) \in R$. Assim, $R = \{(1, 1), (1, 2), (1, 3), (1, 4), (2, 2), (3, 3), (3, 2), (3, 4), (4, 4)\}$ e o diagrama de Hasse associado é



12. Considere o c.p.o. (A, \leq) com o seguinte diagrama de Hasse associado:



- Indique os elementos maximais e minimais de A .
- Seja $X = \{d, e, g, h\}$. Indique o conjunto dos majorantes e o conjunto dos minorantes de X em A e, caso existam, o supremo e o ínfimo de X .
- Seja $Y = \{d, e, g\}$. Indique o conjunto dos majorantes e o conjunto dos minorantes de Y em A e, caso existam, o supremo e o ínfimo de Y .
- Seja $Z = \{b\}$. Indique o conjunto dos majorantes e o conjunto dos minorantes de Z em A e, caso existam, o supremo e o ínfimo de Z .

resolução:

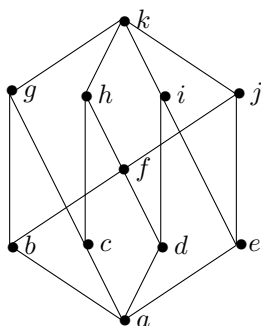
(a) Os elementos maximais são h e j (não existe nenhum elemento x em A tal que $h \leq x$ e não existe nenhum elemento x em A tal que $j \leq x$). Os elementos minimais são a , b e c (não existe nenhum elemento x em A tal que $x \leq a$ ou $x \leq b$ ou $x \leq c$).

(b) Não existe nenhum elemento x em A tal que todos os elementos de X sejam menores ou iguais a x . Logo, $\text{Maj}(X) = \{\}$. Assim, não existe supremo de X . Como b é menor ou igual a todos os elementos de X e não existe mais nenhum elemento em A nessas condições, $\text{Min}(X) = \{b\}$. Temos, conseqüentemente, que $\inf(X) = b$.

(c) Todos os elementos de Y são menores ou iguais (apenas) a g e a j . Logo, $\text{Maj}(Y) = \{g, j\}$. Como os únicos majorantes de Y são g e j e $g \leq j$, segue-se que $\sup(Y) = g$. Sendo b menor ou igual a todos os elementos de Y , e porque não existe mais nenhum elemento em A nessas condições, $\text{Min}(Y) = \{b\}$. Dado que b é o único minorante de Y , $\inf(Y) = b$.

(d) Sabemos que b é menor ou igual a todos os elementos de A , com exceção de a e de c . Logo, $\text{Maj}(Z) = A \setminus \{a, c\}$. O menor dos majorantes de Z é b . Assim, $\sup(Z) = b$. Sendo b um elemento minimal de A , o único elemento x de A tal que $x \leq b$ é o próprio b . Portanto, $\text{Min}(Z) = \{b\}$ e $\inf(Z) = b$.

13. Considere o c.p.o. (A, \leq) com o seguinte diagrama de Hasse associado:



- (a) Seja $X = \{c, d, f, h\}$. Indique o conjunto dos majorantes e o conjunto dos minorantes de X em A e, caso existam, o supremo, o ínfimo, o máximo e o mínimo de X .
- (b) Indique, caso exista, um subconjunto Y de A com um elemento maximal que seja elemento minimal em A .
- (c) Dê exemplo de um subconjunto Z de A com máximo e mínimo diferentes do máximo e do mínimo de A , respetivamente, e tal que $\#Z > 2$.

resolução:

(a) Os elementos m de A para os quais se tem $x \leq m$, para todo $x \in X$, são h e k . Logo, $\text{Maj}(X) = \{h, k\}$. Como $h \leq k$, temos que $\sup(X) = h$. Sendo $\sup(X)$ um elemento de X , segue-se que $\max(X) = h$. O único elemento de A que é menor ou igual a todos os elementos de X é o a . Assim, $\text{Min}(X) = \{a\}$ e, havendo um só minorante de X , é imediato que $\inf(X) = a$. Uma vez que $\inf(X) \notin X$, não existe mínimo de X .

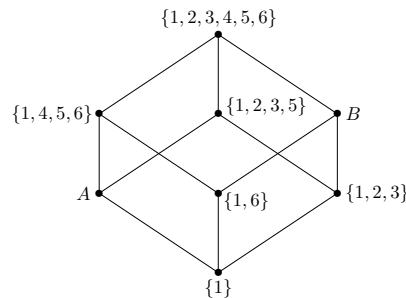
(b) O único elemento minimal de A é o a , que é menor ou igual a todos os outros elementos de A . Assim, para que a seja um elemento maximal de Y , não poderá haver mais nenhum elemento em Y , ou seja, $Y = \{a\}$.

(c) Temos que $\max(A) = k$ e $\min(A) = a$. Seja $Z = \{b, f, j\}$. O mínimo de Z é b e o máximo de Z é j , sendo $\#Z = 3 > 2$. [obs.: há apenas um outro conjunto Z nas condições pretendidas: $Z = \{d, f, h\}$; todos os outros subconjuntos de A com pelo menos três elementos ou não admitem mínimo ou máximo ou têm máximo igual ao máximo de A ou mínimo igual ao mínimo de A .]

14. Dê exemplo de ou justifique por que não existem conjuntos A e B tais que o diagrama abaixo seja o diagrama de Hasse do conjunto parcialmente ordenado

$$(\{\{1\}, A, \{1, 6\}, \{1, 2, 3\}, B, \{1, 2, 3, 5\}, \{1, 4, 5, 6\}, \{1, 2, 3, 4, 5, 6\}\}, \subseteq),$$

em que \subseteq representa a relação de inclusão de conjuntos.



resolução:

Por análise do diagrama, podemos afirmar que $\{1\} \subseteq A$ e que $\{1, 6\} \not\subseteq A$. Assim, $1 \in A$ e $6 \notin A$. Além disso, $A \subseteq \{1, 2, 3, 5\}$ e $A \subseteq \{1, 4, 5, 6\}$. Logo, $A \subseteq \{1, 2, 3, 5\} \cap \{1, 4, 5, 6\}$, ou seja, $A \subseteq \{1, 5\}$. Sendo A distinto de $\{1\}$, segue-se que $A = \{1, 5\}$. Relativamente a B , sabemos, por análise do diagrama, que $\{1, 6\} \subseteq B$ e que $\{1, 2, 3\} \subseteq B$. Portanto, $1, 2, 3, 6$ são elementos de B . Dado que $B \subseteq \{1, 2, 3, 4, 5, 6\}$, poderíamos ainda ter $4 \in B$ ou $5 \in B$ (não ambos, já que $B \neq \{1, 2, 3, 4, 5, 6\}$). Atendendo a que $A \not\subseteq B$, podemos concluir que $5 \notin B$. Podemos considerar $B = \{1, 2, 3, 6\}$ ou $B = \{1, 2, 3, 4, 6\}$.

Capítulo 6

Grafos

Um **grafo** é uma coleção de nós (também designados por vértices) e de arestas. Cada uma das arestas liga dois nós. Para visualizar um grafo, podemos representar os nós por pontos do espaço, do plano ou de qualquer outra superfície e as arestas por linhas que ligam os nós.

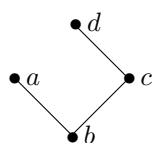
Esta representação não é única. A única característica importante de um grafo é a incidência de nós e arestas. Todos os elementos de um grafo podem sofrer continuamente deslocações ou deformações, continuando, no entanto e sempre, a representar o mesmo grafo, isto é, a mesma coleção de nós e de arestas.

6.1 Grafos simples

[Definição 6.1] Um **grafo simples** G é um par ordenado $G = (V, E)$ no qual V é um conjunto não vazio e E é um conjunto de subconjuntos de V com exactamente dois elementos. Aos elementos de V chamamos **vértices** e aos elementos de E chamamos **arestas**.

[Exemplo]

O grafo



é simples. De facto, se tomarmos $V = \{a, b, c, d\}$ e $E = \{\{a, b\}, \{b, c\}, \{c, d\}\}$, o grafo $G = (V, E)$ tem a representação dada.

Nesta unidade curricular, estudaremos apenas os grafos simples. Não havendo ambiguidade e se nada for dito em contrário, referir-nos-emos aos grafos simples apenas como **grafos**.

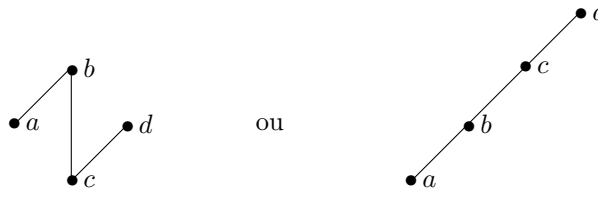
[Definição 6.2] Dois grafos simples $G = (V, E)$ e $G' = (V', E')$ dizem-se **iguais** se $V = V'$ e $E = E'$.

[Observações]

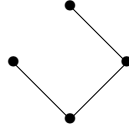
1 | Existem representações *aparentemente* distintas de um mesmo grafo.

No entanto, numa representação de um grafo, o importante é o número de vértices, o número de arestas e o modo como estas se dispõem em relação àqueles.

É claro que o grafo do exemplo anterior pode ser representado por



2 | Uma mesma representação pode descrever grafos que, por definição, são distintos. Por exemplo,



tanto pode representar o grafo $G_1 = (V_1, E_1)$, onde $V_1 = \{a, b, c, d\}$ e $E_1 = \{\{a, b\}, \{b, c\}, \{c, d\}\}$ como o grafo $G_2 = (V_2, E_2)$, onde $V_2 = \{1, 2, 3, 4\}$ e $E_2 = \{\{1, 2\}, \{2, 3\}, \{3, 4\}\}$. Os grafos G_1 e G_2 diferem apenas na natureza dos seus vértices e dizem-se isomorfos.

[Definição 6.3] Dois grafos $G_1 = (V_1, E_1)$ e $G_2 = (V_2, E_2)$ dizem-se **isomorfos** quando existe $f : V_1 \rightarrow V_2$ bijetiva tal que, para todo $v, v' \in V_1$, $\{v, v'\} \in E_1$ se e só se $\{f(v), f(v')\} \in E_2$.

No resto deste estudo não distinguiremos entre grafos isomorfos.

Sejam $n \in \mathbb{N}$ e $m \in \mathbb{N}_0$. Seja $G = (V, E)$ um grafo simples com n vértices e m arestas. Para facilitar a escrita, consideremos

$$V = \{v_i : 1 \leq i \leq n\} \quad \text{e} \quad E = \{e_j : 1 \leq j \leq m\}.$$

[Definição 6.4] Diz-se que $e_j \in E$ é **incidente** com $v_i \in V$ quando existe $v_k \in V$ tal que a aresta e_j liga os vértices v_i e v_k .

[Definição 6.5] Uma matriz $[a_{ij}] \in \mathcal{M}_{n \times m}(\mathbb{Z})$ diz-se uma **matriz de incidência** de G quando

$$a_{ij} = \begin{cases} 0 & \text{se } e_j \text{ não é incidente com } v_i \\ 1 & \text{se } e_j \text{ é incidente com } v_i. \end{cases}$$

[Exemplo]

Seja $G = (V, E)$ o grafo onde $V = \{a, b, c, d\}$ e $E = \{\{a, b\}, \{b, c\}, \{c, d\}\}$. Considerando $v_1 = a$, $v_2 = b$, $v_3 = c$, $v_4 = d$, $e_1 = \{a, b\}$, $e_2 = \{b, c\}$ e $e_3 = \{c, d\}$, obtemos a matriz de incidência

$$M = \begin{bmatrix} 1 & 0 & 0 \\ 1 & 1 & 0 \\ 0 & 1 & 1 \\ 0 & 0 & 1 \end{bmatrix}.$$

Observemos que temos 4 linhas, pois existem 4 vértices, e 3 colunas, correspondentes às 3 arestas.

[Definição 6.6] Dois vértices v_i e v_j de G dizem-se **adjacentes** quando existe uma aresta em G incidente com ambos.

[Definição 6.7] Diz-se que uma matriz $[a_{ij}] \in \mathcal{M}_{n \times n}(\mathbb{Z})$ é uma **matriz de adjacência** de G quando

$$a_{ij} = \begin{cases} 0 & \text{se } v_i \text{ e } v_j \text{ não são adjacentes} \\ 1 & \text{se } v_i \text{ e } v_j \text{ são adjacentes.} \end{cases}$$

[Exemplo]

A matriz

$$M = \begin{bmatrix} 0 & 1 & 0 & 0 \\ 1 & 0 & 1 & 0 \\ 0 & 1 & 0 & 1 \\ 0 & 0 & 1 & 0 \end{bmatrix}$$

é uma matriz de adjacência do grafo referido no exemplo anterior.

[Observações]

1 | Uma matriz de adjacência de um grafo simples é uma matriz quadrada. Mais, é uma matriz simétrica cuja diagonal é preenchida por zeros.

2 | Dado um grafo simples, a construção de uma matriz de incidência (ou de adjacência) depende da ordem pela qual se consideram os vértices e as arestas. Assim, o mesmo grafo admite várias matrizes de incidência e de adjacência. No entanto, duas quaisquer matrizes de incidência (ou de adjacência) de um mesmo grafo são semelhantes, pois uma obtém-se da outra por troca de linhas e/ou colunas.

Existem grafos simples que, pelas suas características próprias, merecem destaque especial.

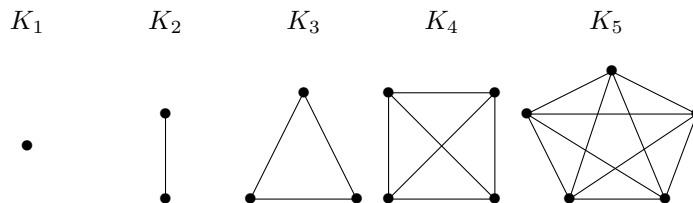
[Definição 6.8] Um **grafo trivial** é um grafo $G = (V, E)$ onde $\#V = 1$ e $\#E = 0$.

[Definição 6.9] Um **grafo nulo** é um grafo $G = (V, E)$ onde $\#E = 0$.

[Definição 6.10] Um **grafo completo** é um grafo no qual dois quaisquer vértices são adjacentes. Um grafo completo com n vértices representa-se por K_n .

[Exemplo]

Para $n = 1, 2, 3, 4, 5$, os grafos completos são

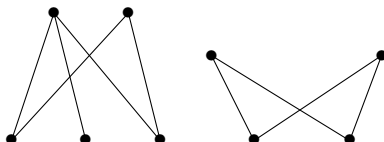


[Proposição 6.11] Um grafo completo K_n tem $\binom{n}{2}$ arestas.

[Definição 6.12] Um grafo $G = (V, E)$ diz-se um **grafo bipartido** se existir uma partição $\{X, Y\}$ de V de tal modo que cada vértice de X é adjacente apenas a vértices de Y e cada vértice de Y é adjacente apenas a vértices de X .

[Exemplo]

Os dois grafos seguintes são bipartidos

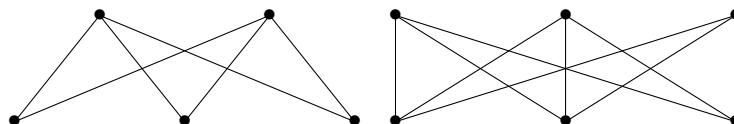


De facto, para cada um dos grafos acima, basta considerar o conjunto X formado pelos dois vértices representados acima e o conjunto Y formado pelos restantes vértices do grafo, representados abaixo dos dois atrás referidos.

[Definição 6.13] Um **grafo bipartido completo** é um grafo bipartido $G = (V, E)$ tal que, para a partição $\{X, Y\}$ de V da definição, cada vértice de X é adjacente a todos os vértices de Y (e, portanto, cada vértice de Y é adjacente a todos os vértices de X). Representa-se um grafo bipartido completo por $K_{m,n}$ onde $\#X = m$ e $\#Y = n$.

[Exemplo]

Os grafos $K_{2,3}$ e $K_{3,3}$ são representados, respetivamente, por



[Definição 6.14] Sejam $G = (V, E)$ um grafo e $v \in V$. Chama-se **grau** (ou **valência**) de v , e representa-se por $\text{grau}(v)$, ao número de arestas incidentes com v .

[Exemplos]

- 1 | No grafo completo K_6 todos os vértices têm grau 5.
- 2 | No grafo bipartido completo $K_{2,3}$ existem dois vértices com grau 3 e três vértices com grau 2.

[Teorema 6.15 (teorema do aperto de mãos)] Num grafo $G = (V, E)$, a soma dos graus de todos os seus vértices é igual ao dobro do número das suas arestas.

[Corolário 6.16] Em qualquer grafo, o número de vértices de grau ímpar é par.

demonstração:

Seja $G = (V, E)$ é um grafo com n arestas. Então,

$$\sum_{\text{grau}(v) \text{ ímpar}} \text{grau}(v) + \sum_{\text{grau}(v) \text{ par}} \text{grau}(v) = \sum_{v \in V} \text{grau}(v) = 2n.$$

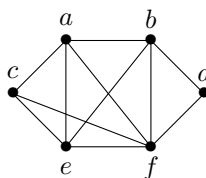
Logo, $\sum_{\text{grau}(v) \text{ ímpar}} \text{grau}(v)$ é par e, portanto, o número de vértices de grau ímpar é par. ■

[Definição 6.17] Um **caminho** num grafo G é uma sequência de vértices de G no qual dois vértices sucessivos definem uma aresta. Representa-se um caminho por $\langle v_1, v_2, \dots, v_k \rangle$, onde v_1, v_2, \dots, v_k são vértices de G . Ao primeiro vértice da sequência chamamos **origem do caminho**, ou **vértice inicial**, e ao último vértice chamamos **destino do caminho**, ou **vértice final**.

Por convenção, chama-se **caminho trivial** à sequência $\langle a \rangle$, onde $a \in V$.

[Exemplo]

No grafo

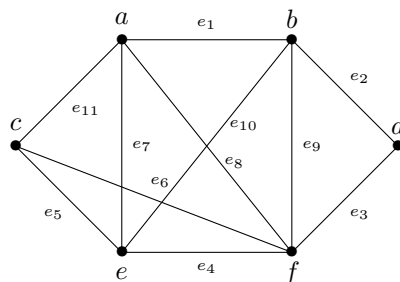


$\langle a, b, d, f, c, e, f, b \rangle$ é um caminho de a a b .

Um caminho pode ser também definido como uma sequência de arestas na qual quaisquer duas arestas sucessivas têm um vértice em comum.

[Exemplo]

No grafo



o caminho $\langle a, b, d, f, c, e, f, b \rangle$ pode também ser representado por $\langle e_1, e_2, e_3, e_6, e_5, e_4, e_9 \rangle$.

[Definição 6.18] Chama-se **comprimento** de um caminho ao número de arestas que definem esse caminho.

[Exemplo]

O caminho apresentado no exemplo anterior tem comprimento 7.

[Definição 6.19] Um **ciclo** é um caminho de comprimento maior que 2 onde não há repetição de vértices, com exceção dos vértices inicial e final, que são iguais.

[Exemplo]

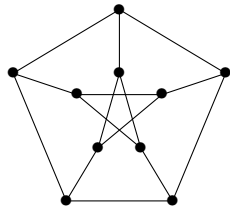
Qualquer linha poligonal pode ser vista como um ciclo.

6.2 Grafos conexos

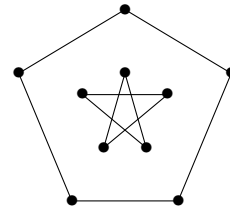
[Definição 6.20] Um **grafo conexo** é um grafo $G = (V, E)$ no qual existe um caminho entre quaisquer dois dos seus vértices. Um **grafo desconexo** é um grafo que não é conexo.

[Exemplo]

O grafo



é um grafo conexo. O grafo

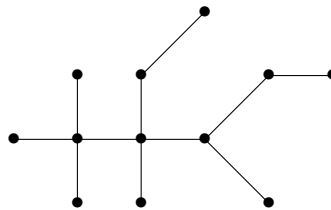


é um grafo desconexo.

[Definição 6.21] Uma **árvore** é um grafo conexo no qual não existem ciclos.

[Exemplo]

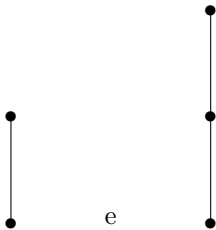
O grafo



é uma árvore.

[Exemplo]

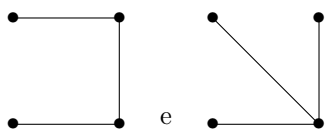
Os grafos



e

são as únicas árvores com 2 e 3 vértices, respetivamente.

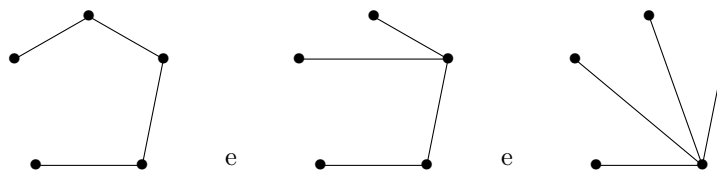
Os grafos



e

são as únicas árvores com 4 vértices.

Os grafos



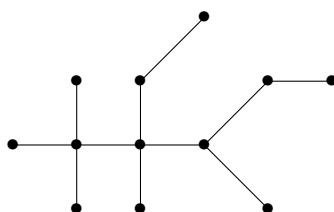
são as únicas árvores com cinco vértices.

[Proposição 6.22] Numa árvore, a diferença entre o número de vértices e o número de arestas é 1.

[Proposição 6.23] Toda a árvore tem pelo menos dois vértices de grau 1.

[Exemplo]

A árvore



tem 12 vértices e 11 arestas.

Existem 7 vértices com grau 1.

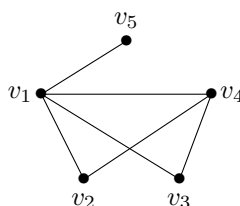
6.3 Exercícios resolvidos

1. Desenhe um grafo que tenha como matriz de incidência a matriz

$$\begin{bmatrix} 1 & 1 & 1 & 1 & 0 & 0 \\ 0 & 0 & 0 & 1 & 1 & 0 \\ 0 & 0 & 1 & 0 & 0 & 1 \\ 0 & 1 & 0 & 0 & 1 & 1 \\ 1 & 0 & 0 & 0 & 0 & 0 \end{bmatrix}.$$

resolução:

Como a matriz dada é do tipo 5×6 , o grafo terá 5 vértices e 6 arestas. Designemos por v_i , para $i = 1, \dots, 5$, os vértices do grafo e por e_i , para $i = 1, \dots, 6$, as suas arestas. Atendendo às entradas da primeira coluna, sabemos que a aresta e_1 liga os vértices v_1 e v_5 , uma vez que as únicas entradas da primeira coluna que são não nulas são as da primeira e da quinta linhas. De modo análogo, podemos inferir que e_2 liga v_1 e v_4 , e_3 liga v_1 e v_3 , e_4 liga v_1 e v_2 , e_5 liga v_2 e v_4 e e_6 liga v_3 e v_4 . Obtemos o seguinte grafo:

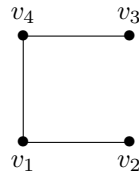


2. Desenhe um grafo que tenha como matriz de adjacência a matriz

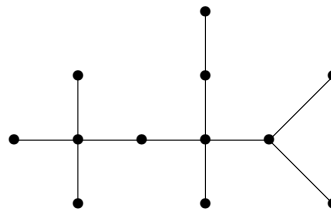
$$\begin{bmatrix} 0 & 1 & 0 & 1 \\ 1 & 0 & 0 & 0 \\ 0 & 0 & 0 & 1 \\ 1 & 0 & 1 & 0 \end{bmatrix}.$$

resolução:

Como a matriz dada é do tipo 4×4 , o grafo terá 4 vértices. Designemos por v_i , para $i = 1, \dots, 4$, esses vértices. Atendendo às entradas da primeira linha, sabemos que o vértice v_1 é adjacente com v_2 (pois a entrada na posição $(1,2)$ é 1) e com v_4 (pois a entrada na posição $(1,4)$ é 1). Além disso, o vértice v_1 não é adjacente com v_3 (a entrada na posição $(1,3)$ é 0). De modo análogo, podemos inferir que v_2 apenas é adjacente com v_1 , que v_3 apenas é adjacente com v_4 e que v_4 é adjacente com v_1 e v_3 . Obtemos o seguinte grafo:

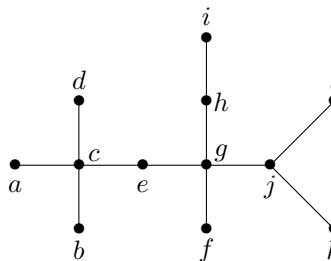


3. Mostre que o seguinte grafo é bipartido:



resolução:

Consideremos a seguinte etiquetagem dos vértices:



Determinemos uma partição $\{X, Y\}$ do conjunto de vértices $\{a, b, c, d, e, f, g, h, i, j, k, l\}$ de tal modo que cada vértice de X seja adjacente apenas a vértices de Y e cada vértice de Y seja adjacente apenas a vértices de X .

Começemos por fixar que o vértice a está em X . Então, o vértice c , que é adjacente com a , tem de pertencer a Y .

Deste modo, os vértices b , d e e , que são adjacentes com c , têm de pertencer a X .

Sendo e um elemento de X e sendo g adjacente com e , segue-se que $g \in Y$. Logo, os vértices f , h e j , que são adjacentes com g , têm de pertencer a X .

Como $h \in X$ e i é adjacente com h , i tem de pertencer a Y .

Finalmente, dado que $j \in X$ e dado que k e l são adjacentes com j , segue-se que k e l têm de pertencer a Y .

Obtemos, assim, a partição $\{\{a, b, d, e, f, h, j\}, \{c, g, i, k, l\}\}$ que nos permite afirmar que o grafo dado é bipartido.

4. Dê exemplo, caso exista, de:

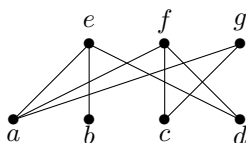
- (a) um grafo com exactamente um vértice de grau par.
- (b) um grafo bipartido com 7 vértices.
- (c) um grafo que contenha um ciclo de comprimento 5.
- (d) um grafo conexo com 2 vértices de grau 3, 3 vértices de grau 2 e 1 vértice de grau 1.

resolução:

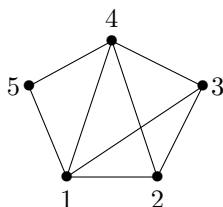
- (a) O grafo trivial (um vértice e zero arestas) satisfaz a condição enunciada:

•

- (b) O seguinte grafo $G = (V, E)$ é bipartido uma vez que $\{\{a, b, c, d\}, \{e, f, g\}\}$ é uma partição de V tal que cada vértice de $\{a, b, c, d\}$ é adjacente apenas a vértices de $\{e, f, g\}$ e cada vértice de $\{e, f, g\}$ é adjacente apenas a vértices de $\{a, b, c, d\}$.



- (c) O caminho $\langle 1, 2, 3, 4, 5, 1 \rangle$ é um ciclo com comprimento 5 no grafo seguinte:



- (d) Em qualquer grafo simples, o número de vértices de grau ímpar é par. Logo, não existe um grafo que satisfaça as condições pedidas (pois tendo 2 vértices de grau 3 e 1 de grau 1, teria 3 vértices de grau ímpar).

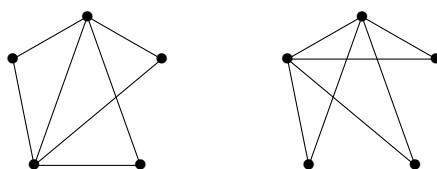
5. Sobre um dado grafo G sabe-se que tem exatamente 5 vértices e 8 arestas. Qual das seguintes afirmações é necessariamente verdadeira?

- (a) É possível todos os vértices de G terem o mesmo grau.
- (b) Se exatamente dois dos vértices de G têm grau 4, então G tem dois vértices de grau ímpar.
- (c) G é uma árvore.

resolução:

(a) Sabemos que a soma dos graus de todos os vértices é igual ao dobro do número de arestas. Logo, a soma dos graus será 16. Para os cinco vértices terem o mesmo grau, a soma dos graus teria de ser um múltiplo de 5, o que não acontece. Portanto, a afirmação é falsa.

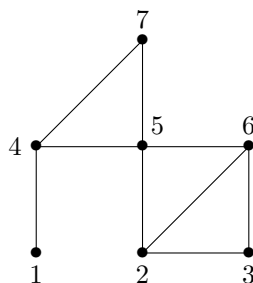
(b) Se dois vértices têm grau 4, cada um deles é adjacente a todos os outros. Sendo assim, existem 7 arestas incidentes com alguns desses dois vértices. Os casos possíveis são, a menos de isomorfismo, e para essas 7 arestas:



Tendo o grafo 8 arestas, haverá uma outra aresta incidente com dois dos outros vértices. Assim, dois dos outros vértices terão grau 3 e o outro grau 2. Há portanto, dois vértices de grau ímpar em G e a afirmação é verdadeira.

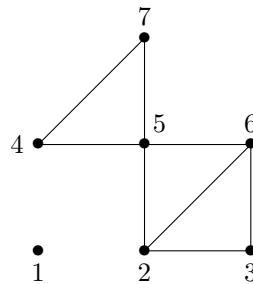
(c) Numa árvore, a diferença entre o número de vértices e o número de arestas é 1, o que não acontece em G e, por isso, a afirmação é falsa.

6. Um conjunto de desconexão de um grafo conexo G é um conjunto de arestas cuja remoção dá origem a um grafo desconexo. Encontre conjuntos de desconexão para o seguinte grafo com 1 e 2.



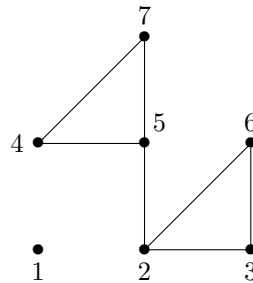
resolução:

Consideremos o conjunto $\{\{1, 4\}\}$ formado pela aresta que incidente com os vértices 1 e 4. A remoção dessa aresta dá origem ao grafo

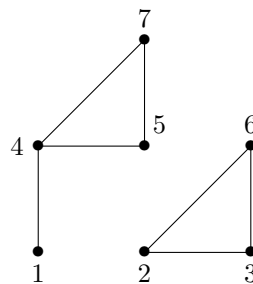


que é desconexo (não há nenhum caminho do vértice 1 para qualquer outro dos vértices). Note-se que não há mais nenhum conjunto de desconexão apenas com uma aresta.

É claro que se removermos a aresta $\{1, 4\}$ e ainda outra aresta qualquer, continuaremos a obter um grafo desconexo. Por isso, um conjunto de desconexão com duas arestas pode ser $\{\{1, 4\}, \{5, 6\}\}$. O gráfico obtido removendo estas arestas é



Note-se, contudo que há outros conjuntos de desconexão com duas arestas que não incluem a aresta $\{1, 4\}$. Removendo, por exemplo, as arestas $\{5, 2\}$ e $\{5, 7\}$, obtemos o grafo



que é desconexo, uma vez que não existem caminhos, por exemplo, do vértice 2 para o vértice 5. Logo, $\{\{5, 2\}, \{5, 6\}\}$ é um conjunto de desconexão com duas arestas.